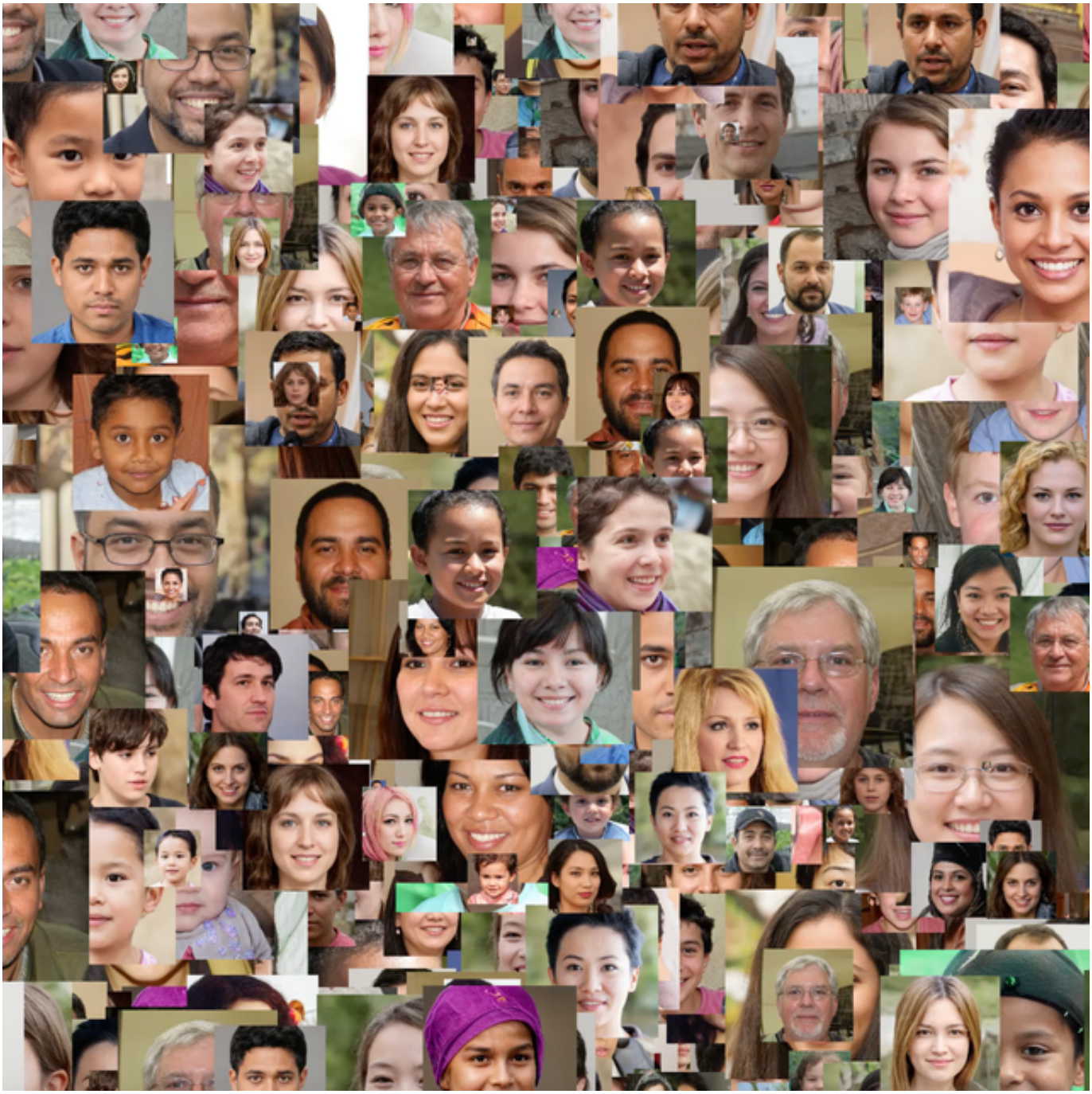
The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and “might lead to a dystopian future or something,” a backer says.

Published Jan. 18, 2020Updated Nov. 2, 2021





Adam Ferriss

Until recently, Hoan Ton-That's greatest hits included an obscure iPhone game and an app that let people put Donald Trump's distinctive yellow hair

on their own photos.

Then Mr. Ton-That — an Australian techie and onetime model — did something momentous: He invented a tool that could end your ability to walk down the street anonymously, and provided it to hundreds of law enforcement agencies, ranging from local cops in Florida to the F.B.I. and the Department of Homeland Security.

His tiny company, Clearview AI, devised a groundbreaking facial recognition app. You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared. The system — whose backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites — goes far beyond anything ever constructed by the United States government or Silicon Valley giants.

Federal and state law enforcement officers said that while they had only limited knowledge of how Clearview works and who is behind it, they had used its app to help solve shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases.

Until now, technology that readily identifies everyone based on his or her face has been taboo because of its radical erosion of privacy. Tech companies capable of releasing such a tool have refrained from doing so; in 2011, Google's chairman at the time said it was the one technology the company had held back because it could be used "in a very bad way." Some large cities, including San Francisco, have barred police from using facial recognition technology.

But without public scrutiny, more than 600 law enforcement agencies have started using Clearview in the past year, according to the company, which declined to provide a list. The computer code underlying its app, analyzed by The New York Times, includes programming language to pair it with augmented-reality glasses; users would potentially be able to identify every

person they saw. The tool could identify activists at a protest or an attractive stranger on the subway, revealing not just their names but where they lived, what they did and whom they knew.

And it's not just law enforcement: Clearview has also licensed the app to at least a handful of companies for security purposes.

"The weaponization possibilities of this are endless," said Eric Goldman, co-director of the High Tech Law Institute at Santa Clara University. "Imagine a rogue law enforcement officer who wants to stalk potential romantic partners, or a foreign government using this to dig up secrets about people to blackmail them or throw them in jail."

Clearview has shrouded itself in secrecy, avoiding debate about its boundary-pushing technology. When I began looking into the company in November, its website was a bare page showing a nonexistent Manhattan address as its place of business. The company's one employee listed on LinkedIn, a sales manager named "John Good," turned out to be Mr. Ton-That, using a fake name. For a month, people affiliated with the company would not return my emails or phone calls.

While the company was dodging me, it was also monitoring me. At my request, a number of police officers had run my photo through the Clearview app. They soon received phone calls from company representatives asking if they were talking to the media — a sign that Clearview has the ability and, in this case, the appetite to monitor whom law enforcement is searching for.

Facial recognition technology has always been controversial. It makes people nervous about Big Brother. It has a tendency to deliver false matches for certain groups, like people of color. And some facial recognition products used by the police — including Clearview's — haven't been vetted by independent experts.

Clearview's app carries extra risks because law enforcement agencies are

uploading sensitive photos to the servers of a company whose ability to protect its data is untested.

The company eventually started answering my questions, saying that its earlier silence was typical of an early-stage start-up in stealth mode. Mr. Ton-That acknowledged designing a prototype for use with augmented-reality glasses but said the company had no plans to release it. And he said my photo had rung alarm bells because the app "flags possible anomalous search behavior" in order to prevent users from conducting what it deemed "inappropriate searches."

In addition to Mr. Ton-That, Clearview was founded by Richard Schwartz — who was an aide to Rudolph W. Giuliani when he was mayor of New York — and backed financially by Peter Thiel, a venture capitalist behind Facebook and Palantir.

Another early investor is a small firm called Kirenaga Partners. Its founder, David Scalzo, dismissed concerns about Clearview making the internet searchable by face, saying it's a valuable crime-solving tool.

"I've come to the conclusion that because information constantly increases, there's never going to be privacy," Mr. Scalzo said. "Laws have to determine what's legal, but you can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it."

Hoan Ton-That, founder of Clearview AI, whose app matches faces to images it collects from across the internet.Amr Alfiky for The New York Times

Addicted to A.I.

Mr. Ton-That, 31, grew up a long way from Silicon Valley. In his native Australia, he was raised on tales of his royal ancestors in Vietnam. In 2007, he dropped out of college and moved to San Francisco. The iPhone had just arrived, and his goal was to get in early on what he expected would be a vibrant market for social media apps. But his early ventures never gained real traction.

In 2009, Mr. Ton-That created a site that let people share links to videos with all the contacts in their instant messengers. Mr. Ton-That shut it down after it was branded a "phishing scam." In 2015, he spun up Trump Hair, which added Mr. Trump's distinctive coif to people in a photo, and a photo-sharing program. Both fizzled.

Dispirited, Mr. Ton-That moved to New York in 2016. Tall and slender, with

long black hair, he considered a modeling career, he said, but after one shoot he returned to trying to figure out the next big thing in tech. He started reading academic papers on artificial intelligence, image recognition and machine learning.

Mr. Schwartz and Mr. Ton-That met in 2016 at a book event at the Manhattan Institute, a conservative think tank. Mr. Schwartz, now 61, had amassed an impressive Rolodex working for Mr. Giuliani in the 1990s and serving as the editorial page editor of The New York Daily News in the early 2000s. The two soon decided to go into the facial recognition business together: Mr. Ton-That would build the app, and Mr. Schwartz would use his contacts to drum up commercial interest.

Police departments have had access to facial recognition tools for almost 20 years, but they have historically been limited to searching government-provided images, such as mug shots and driver's license photos. In recent years, facial recognition algorithms have improved in accuracy, and companies like Amazon offer products that can create a facial recognition program for any database of images.

Mr. Ton-That wanted to go way beyond that. He began in 2016 by recruiting a couple of engineers. One helped design a program that can automatically collect images of people's faces from across the internet, such as employment sites, news sites, educational sites, and social networks including Facebook, YouTube, Twitter, Instagram and even Venmo. Representatives of those companies said their policies prohibit such scraping, and Twitter said it explicitly banned use of its data for facial recognition.

Another engineer was hired to perfect a facial recognition algorithm that was derived from academic papers. The result: a system that uses what Mr. Ton-That described as a "state-of-the-art neural net" to convert all the images into mathematical formulas, or vectors, based on facial geometry — like how far apart a person's eyes are. Clearview created a vast directory that

clustered all the photos with similar vectors into “neighborhoods.” When a user uploads a photo of a face into Clearview’s system, it converts the face into a vector and then shows all the scraped photos stored in that vector’s neighborhood — along with the links to the sites from which those images came.

Mr. Schwartz paid for server costs and basic expenses, but the operation was bare bones; everyone worked from home. “I was living on credit card debt,” Mr. Ton-That said. “Plus, I was a Bitcoin believer, so I had some of those.”

Mr. Ton-That showing the results of a search for a photo of himself. Amr Alfiky for The New York Times

Going Viral With Law Enforcement

By the end of 2017, the company had a formidable facial recognition tool, which it called Smartcheckr. But Mr. Schwartz and Mr. Ton-That weren’t sure whom they were going to sell it to.

Maybe it could be used to vet babysitters or as an add-on feature for surveillance cameras. What about a tool for security guards in the lobbies of buildings or to help hotels greet guests by name? “We thought of every idea,” Mr. Ton-That said.

One of the odder pitches, in late 2017, was to Paul Nehlen — an anti-Semite and self-described “pro-white” Republican running for Congress in Wisconsin — to use “unconventional databases” for “extreme opposition research,” according to a document provided to Mr. Nehlen and later posted online. Mr. Ton-That said the company never actually offered such services.

The company soon changed its name to Clearview AI and began marketing to law enforcement. That was when the company got its first round of funding from outside investors: Mr. Thiel and Kirenaga Partners. Among other things, Mr. Thiel was famous for secretly financing Hulk Hogan’s

lawsuit that bankrupted the popular website Gawker. Both Mr. Thiel and Mr. Ton-That had been the subject of negative articles by Gawker.

“In 2017, Peter gave a talented young founder $200,000, which two years later converted to equity in Clearview AI,” said Jeremiah Hall, Mr. Thiel’s spokesman. “That was Peter’s only contribution; he is not involved in the company.”

Even after a second funding round in 2019, Clearview remains tiny, having raised $7 million from investors, according to Pitchbook, a website that tracks investments in start-ups. The company declined to confirm the amount.

In February, the Indiana State Police started experimenting with Clearview. They solved a case within 20 minutes of using the app. Two men had gotten into a fight in a park, and it ended when one shot the other in the stomach. A bystander recorded the crime on a phone, so the police had a still of the gunman’s face to run through Clearview’s app.

They immediately got a match: The man appeared in a video that someone had posted on social media, and his name was included in a caption on the video. “He did not have a driver’s license and hadn’t been arrested as an adult, so he wasn’t in government databases,” said Chuck Cohen, an Indiana State Police captain at the time.

The man was arrested and charged; Mr. Cohen said he probably wouldn’t have been identified without the ability to search social media for his face. The Indiana State Police became Clearview’s first paying customer, according to the company. (The police declined to comment beyond saying that they tested Clearview’s app.)

Clearview deployed current and former Republican officials to approach police forces, offering free trials and annual licenses for as little as $2,000. Mr. Schwartz tapped his political connections to help make government

officials aware of the tool, according to Mr. Ton-That. ("I'm thrilled to have the opportunity to help Hoan build Clearview into a mission-driven organization that's helping law enforcement protect children and enhance the safety of communities across the country," Mr. Schwartz said through a spokeswoman.)

The company's main contact for customers was Jessica Medeiros Garrison, who managed Luther Strange's Republican campaign for Alabama attorney general. Brandon Fricke, an N.F.L. agent engaged to the Fox Nation host Tomi Lahren, said in a financial disclosure report during a congressional campaign in California that he was a "growth consultant" for the company. (Clearview said that it was a brief, unpaid role, and that the company had enlisted Democrats to help market its product as well.)

A chart from marketing materials that Clearview provided to law enforcement.Clearview

The company's most effective sales technique was offering 30-day free trials to officers, who then encouraged their acquisition departments to sign up and praised the tool to officers from other police departments at conferences and online, according to the company and documents provided by police departments in response to public-record requests. Mr. Ton-That finally had his viral hit.

In July, a detective in Clifton, N.J., urged his captain in an email to buy the software because it was "able to identify a suspect in a matter of seconds." During the department's free trial, Clearview had identified shoplifters, an Apple Store thief and a good Samaritan who had punched out a man threatening people with a knife.

Photos "could be covertly taken with telephoto lens and input into the software, without 'burning' the surveillance operation," the detective wrote in the email, provided to The Times by two researchers, Beryl Lipton of MuckRock and Freddy Martinez of Open the Government. They discovered Clearview late last year while looking into how local police departments are

using facial recognition.

According to a Clearview sales presentation reviewed by The Times, the app helped identify a range of individuals: a person who was accused of sexually abusing a child whose face appeared in the mirror of someone's else gym photo; the person behind a string of mailbox thefts in Atlanta; a John Doe found dead on an Alabama sidewalk; and suspects in multiple identity-fraud cases at banks.

Listen to 'The Daily': The End of Privacy as We Know It?

An unregulated facial recognition app can probably tell the police your name, and help them find out where you live and who your friends are.

transcript

Hosted by Michael Barbaro; produced by Annie Brown and Daniel Guillemette; with help from Michael Simon Johnson; and edited by Paige Cowett and Larissa Anderson

An unregulated facial recognition app can probably tell the police your name, and help them find out where you live and who your friends are.

[music]
michael barbaro

> From The New York Times, I'm Michael Barbaro. This is "The Daily."
>
> Today: A secretive company promising the next generation of facial recognition software has compiled a database of images far bigger than anything ever constructed by the U.S. government. The Daily's Annie Brown speaks to reporter Kashmir Hill about whether the technology is a breakthrough for law enforcement or the end of privacy as we know it.
>
> It's Monday, February 10.

annie brown

> Kashmir, how did this story come to you?

kashmir hill

> So I got an email. It was a Wednesday morning. I was checking my phone. And it was from a tipster who had gotten a bunch of documents from police departments. And one of the police departments had sent along this memo about a private company that was offering a radical new tool to solve crimes using facial recognition.

annie brown

> And what would make a facial recognition tool radical?

kashmir hill

So law enforcement has for years had access to facial recognition tools. But what this company was offering was unlike any other facial recognition tools that police have been using, because they had scraped the open web of public photos — from Facebook, from Venmo, from Twitter, from education sites, employment sites — and had a massive database of billions of photos. So the pitch is that you can take a picture of a criminal suspect, put their face into this app and identify them in seconds.

annie brown

And when you read this memo, what do you make of what this company is offering?

kashmir hill

So I've been covering privacy for 10 years, and I know that a technology like this in public hands is the nightmare scenario.

[music]

This has been a tool that was too taboo for Silicon Valley giants who were capable of building it. Google in 2011 said that they could release a tool like this, but it was the one technology they were holding back because it could be used in a very bad way.

annie brown

And why exactly is this kind of technology this line in the sand that no one will cross? What makes it so dangerous?

kashmir hill

So imagine this technology in public hands. It would mean that if you were at a bar and someone saw you and was interested in you, they could take your photo, run your face through the app, and then it pulls up all these photos of you from the internet. It probably takes them back to your Facebook page. So now they know your name, they know who you're friends with, they can Google your name, they can see where you live, where you work, maybe how much money you make. Let's say you're a parent and you're walking down the street with your three-year-old. Somebody can take a photo of you and know where the two of you live. Imagine you're a protester in the U.S. or in a more authoritarian regime. All of a sudden they know everything about you, and you can face repercussions for just trying to exercise your political opinions. If this app were made publicly available, it would be the end of being anonymous in public. You would have to assume anyone can know who you are any time they're able to take a photo of your face.

annie brown

And so that technology is what this company is pitching these police departments?

kashmir hill

Exactly.

annie brown

And what do you know about this company at this point?

kashmir hill

So at this point, all I really know is that the company is called Clearview AI. And so the first thing I do is Google it. And I find their website, which is clearview.ai. And the website is pretty bare, but there's also an office address listed there, 145 West 41st Street, which happens to be just a couple of blocks from The New York Times office.

annie brown

Right.

kashmir hill

So I decided to walk over there, and there just is no 145 West 41st Street. So that was weird. So now I have this company that's offering this radical new tool —

annie brown

It's got a fake address.

kashmir hill

It's got a fake address, which is a huge red flag.

annie brown

So what you do next?

kashmir hill

I found the company on LinkedIn. It only had one employee listed, a sales manager named John Good, which —

annie brown

John Good.

kashmir hill

John Good. It seemed like it could also be fake. And I sent that person a LinkedIn message and never heard back. So one of the things I find online is a website called PitchBook that lists investments in start-ups. And so it says that this Clearview AI has received $7 million from a venture capital firm and from Peter Thiel — you know, a big name in Silicon Valley, invested in Facebook and Palantir. So I reach out to his spokesperson, and he says I'll get back to you. I never hear from him again. And then one day, I open up Facebook, and I have a message from a friend whose name I don't recognize. And he says, hey, I hear you're looking into Clearview AI. I know them. They're a great company. How can I help?

annie brown

And you don't know who this guy is?

kashmir hill

I don't. I mean, it's a guy I met once 10 years ago. And somehow he knows that I'm looking into this company. But I'll take it. You know, finally —

annie brown

Right!

kashmir hill

— somebody wants to talk to me about Clearview AI. And so I say, hey, can I give you a call? And then he doesn't respond, which I'm getting used to.

annie brown

You just can't catch a break.

kashmir hill

I know. I'm like, I cannot believe this is another dead end.

So phone and email are not working for me. So I just need to figure out another door to knock on to try to talk to a real human being. And one of the investors in the company is this venture capital firm that has an office in Bronxville, New York. So on a cold, rainy Tuesday, I got on the train and headed to Bronxville. I get to the company's address. It's just like in a retail space. And go inside. There's this long, quiet hallway of office suites, and this venture capital firm is at the very end. And I knock on the door, and there's no one there. So I start trying to talk to their neighbors, and a woman who works next door says, oh yeah, they're never here. So I'm walking down the stairs to go back out of the building, and two guys walk through the door. They're both in dark suits with lavender and pink shirts underneath, and they just kind of look like V.C.s to me. So I say, hey, are you with this venture capital firm? And they say, we are. Who are you? And I was like, I'm the New York Times reporter who's been trying to get in touch with you. And they said, the company has told us not to talk to you. And I said, well I've come all the way out to Bronxville. Can we just chat for a little bit? And they say, O.K. If probably helps that I'm very pregnant, and they offered me water. And they just start telling me everything.

[music]

annie brown

And what do they tell you?

kashmir hill

They confirm that they've invested in Clearview AI and that Peter Thiel has also invested. They identified the genius coder behind the company, this guy named Hoan Ton-That. And they say he's Vietnamese royalty but he's from Australia. And they also tell me that Hoan is the one that was using the fake name John Good on LinkedIn.

annie brown

He's John Good.

kashmir hill

He's John Good.

And they confirm that law enforcement is already using the app. And that law enforcement loves it and that it's spreading like wildfire.

annie brown

Wow.

kashmir hill

So I've learned some stuff from these two investors, but no one from the company is talking to me still. So in the meantime, I am also reaching out to law enforcement, because I want to know if this app really works as well as the company claims. By this point, I had learned that over 600 law enforcement agencies had tried the app, including the Department of Homeland Security and the F.B.I.

annie brown

Wow. It's not just local police departments. This is being used by the federal government already.

kashmir hill

Yeah, I mean, I was just shocked to discover how easily government agencies can just try a new technology without apparently knowing much about the company that provides it. So I talked to a retired police chief from Indiana, who was actually one of the first departments to use the app. And they solved a case within 20 seconds, he said.

annie brown

A case they hadn't been able to solve?

kashmir hill

That they hadn't been able to solve. One of the officers told me that he went back through like 30 dead-end cases that hadn't had any hits on the government database, and he got a bunch of hits using the app. So they were really excited about it.

annie brown

This is way more effective than what they were using before.

kashmir hill

Exactly. With the government databases they were previously using, they had to have a photo that was just a direct full-face photo of a suspect — like mug shots and driver's license photos. But with Clearview, it could be a person wearing glasses, or a hat, or part of their face was covered, or they were in profile, and officers were still getting results on these photos.

annie brown

Wow.

kashmir hill

But the most astounding story I was told was that investigators had this child exploitation video, and there was an adult who was visible in the video just for a few seconds in the background. So they had this person's face. They had run it through their usual databases and not gotten anything back. But then they ran his face through Clearview's app, and he turned up in the background of someone else's gym selfie. You could see his face in the mirror. And so they figured out what gym this photo was taken out. They went to the gym. They asked the employees, do you know who this is? And the employee said, we can't tell you. We have to protect our members' privacy. But then later, the detectives got a text from

somebody who worked there identifying the person. And that — I mean, that's just something that would not have been possible without Clearview's app.

So because officers were telling me the tool works so well, I wanted to see it for myself, on myself. And I asked them if they would run my photo through the app. But every time I did this, things would get weird. The officers would tell me that they ran my photo and there were no results.

annie brown

No pictures of you?

kashmir hill

There were no pictures of me, which was really weird, because I have a lot of photos of myself online. And then officers would just stop responding to me or talking to me. And I had no idea what was going on until one officer was kind enough to explain to me.

[phone ringing]

officer

Hello, how are you.

kashmir hill

Hey. It's Kashmir.

officer

Yes, hi. Mm-hmm.

kashmir hill

I'm keeping this officer anonymous because he could get in serious trouble for talking to me so openly about Clearview.

kashmir hill

If you could just describe yourself, to the extent that you can describe yourself.

officer

I'm a police officer at a large metropolitan police department.

kashmir hill

So he's a cop who was doing a 30-day free trial of the app. And he was really impressed with it. So I asked him if he wouldn't mind running my photo.

annie brown

And what did he tell you happened when he sent your picture through?

officer

Yeah, nothing. I didn't get a response at all.

kashmir hill

No results?

officer

No results. And within a couple of minutes of me putting your photo up there — maybe five, less than 10 — I got a phone call from the Clearview company. They wanted to know why I was uploading a New York Times reporter's photo.

kashmir hill

That is so wild. I don't know. [LAUGHS] It creeps me out as a reporter. I mean yeah, it just —

officer

It kind of creeped me out as a user.

kashmir hill

So this implied that Clearview flagged my face in their system such that they got an alert when a police officer ran my face. Which I found —

annie brown

Wow.

kashmir hill

— very alarming, because this is telling me for the first time that this company is able to monitor who law enforcement is looking for, and not just know who they're looking for, but manipulate the results. And so then that made me go back to the earlier officers who had run my photo. And they all confirmed, yes, I got a call from the company, and they said, we're not supposed to be talking to the media.

[music]

kashmir hill

So were you able to keep using the app after that?

officer

My account was deactivated.

kashmir hill

Did you ever get access back?

officer

I never did. But I have colleagues that have access. So if I were to need a picture searched, I could just email it to them and they can email me the results.

kashmir hill

And you think the trade-offs are worth it, in terms of what the company has access to?

officer

Do I think it's worth it? So from a law enforcement perspective, it's worth it. We get a lot of cases, and we don't usually have a lot of leads. And so anything that can — honestly,

anything that can help us solve a crime is a win for us. From a privacy perspective, it's rather frightening the amount of information that they were able to get and provide. As long as they're doing it for the right reasons, then everything will work out. Let's put it that way.

[music]

kashmir hill

But the problem is we don't know anything about the company at this point. We don't know if there's any kind of oversight. We don't know who the people are that are operating this and what their intentions are with their product. The person in charge of the company won't talk to me. But then, it's the end of December when I get a call from the company's spokeswoman. And she says that the founder, Hoan Ton-That, is ready to talk.

michael barbaro

We'll be right back.

kashmir hill

Do you have a hard stop?

hoan ton-that

No I don't actually. 12:30.

lisa linden

12:00 noon.

hoan ton-that

Oh, 12:00 noon.

kashmir hill

I have no hard stop.

lisa linden

Oh.

kashmir hill

And I have lots of questions, so I'll take as much time as you can give me.

annie brown

So Kashmir, you finally got an interview with the founder of Clearview, this man named Hoan Ton-That. Where do you meet him?

kashmir hill

So we met in a WeWork in Chelsea. He came down to the lobby.

kashmir hill

You like New York, you're going to stay here?

hoan ton-that

Oh, yeah.

kashmir hill

And his appearance surprised me, because I had Googled him online and there are a lot of photos of him. And he's usually pretty eccentric — like a lot of paisley shirts, he's at Burning Man.

hoan ton-that

Let's go to the back room.

kashmir hill

But in person he was very conservative. He was in this dark blue navy suit with a white button-up and leather shoes. So he looked very much like the security start-up entrepreneur.

annie brown

He was looking the part.

kashmir hill

He was looking the part.

kashmir hill

When were you born? How old are you?

hoan ton-that

'88, so I'm 31.

kashmir hill

O.K.

annie brown

And what do you learn about him?

kashmir hill

So he is 31. He grew up in Australia, but you can't hear that in his voice.

hoan ton-that

I love computers, obviously.

kashmir hill

Yeah, so how did you get interested in technology?

hoan ton-that

We had a computer, of course, when I was four or five years old.

kashmir hill

So his family got a computer when he was three or four, and he was always tinkering with

computers growing up.

hoan ton-that

We got the internet when I was 10, I think. And then you could discover all these things online. But Linux, I was like I have to get this thing. It's the nerdiest thing ever. I convinced my dad. We installed it, and I would spend the whole summer reinstalling and learning Linux stuff, staying home from high school and learning programming for fun. So that's — I just really liked it.

kashmir hill

He enrolled in college, decided to drop out like many technologists do, and moved to San Francisco when he was 19.

hoan ton-that

— 2007, before it was a big thing, right? It was kind of getting there, but it wasn't huge.

kashmir hill

This is 2007, and this is kind of a boom time. The iPhone has just come out.

hoan ton-that

That's the Facebook app era. Remember that?

kashmir hill

Yeah.

kashmir hill

People are becoming millionaires by making Facebook games. And he wants to be the next big app guy.

hoan ton-that

Being there is a lot different from reading about it online. You absorb a lot more of how people get things done. And you learn a lot more secrets.

annie brown

What did he built?

kashmir hill

So the Facebook apps were like "would you rather" apps and kind of like romantic GIFs.

hoan ton-that

Did Some of the first iPhone games as well.

kashmir hill

One of his most recent apps was called Trump Hair, and it was an app for adding Trump's

hair to your photos.

annie brown

That's it?

kashmir hill

That's it. The tagline was, "It's gonna be yuge!"

annie brown

O.K. [LAUGHS] So how do you move from a Donald Trump hair app to something that seems like it could revolutionize police work?

kashmir hill

Well, he moved to New York. And that seemed to be a big change for him. And he started meeting very different people. And one of the most important people he met was Richard Schwartz.

hoan ton-that

I ended up meeting Richard at a party.

kashmir hill

This 61-year-old guy who worked for Mayor Rudy Giuliani in the 1990s. He was just very politically connected.

hoan ton-that

I really loved that. He had a lot of stories. And then we talked for an hour about different ideas. Because I was like, this is what I do — technology. I can make anything. And it went from there.

kashmir hill

And the two of them decided, with Hoan Ton-That's tech know-how and Richard's Rolodex, that they want to try to start a facial recognition company together.

annie brown

And why facial recognition? Why did the two of them choose that?

kashmir hill

I think it was because Hoan had started reading a lot of papers about facial recognition and machine learning.

hoan ton-that

I had never really studied AI stuff before, but I could pick up a lot of it.

kashmir hill

And I think they realized they could make money doing it.

kashmir hill

What would you say, in terms of the range of ideas at first, what were you thinking?

hoan ton-that

A lot. I could go on, really crazy, but —

kashmir hill

There's a lot of face recognition algorithms out there, and a lot that work pretty well. What was different about what Hoan Ton-That and Richard Schwartz were doing is they had been willing to scrape all of these photos from the internet. So they just had a huge database of photos.

annie brown

Right, the billions of photos.

kashmir hill

Exactly.

hoan ton-that

And then we had this point where we got to 99 percent accuracy. I remember that, it was just in the office. And he was like, wow, it works. Try that one again. Try that one again. And just every time, it would pick the right person out. And that's when we knew, this is crazy. This actually works.

annie brown

Is that legal? Can you just take photographs from anywhere on the internet and use them for this kind of thing?

kashmir hill

There was a ruling in a federal court this fall that said, yeah, this kind of public scraping seems to be legal.

annie brown

And what are they hoping to do with this software at this point?

kashmir hill

I mean, they're just trying to figure out how they can make money off of the app. And so they eventually end up settling on law enforcement.

hoan ton-that

And they start solving cases from grainy A.T.M. photos, cases they would've never solved. So this spread to different departments, and then from one agency to other agencies.

annie brown

And do you ask him about that thing that happened with the officer who couldn't find your photos?

kashmir hill

Yeah, so that was one of my questions, and I wasn't entirely satisfied by his answer.

hoan ton-that

So —

kashmir hill

One thing that surprised me — some of the officers I talked to tried to run my photo through it, and they got no hits. And I tons of photos online.

hoan ton-that

[LAUGHS] It must have been a bug.

kashmir hill

Did you guys block me from like getting results?

hoan ton-that

I don't know about that.

kashmir hill

Because I was like, this doesn't make any sense.

kashmir hill

He said, oh yeah, that was a software bug. But he laughed.

kashmir hill

I was like, I have 1,000 photos online. This can't work as well as they say it works.

hoan ton-that

Yeah, well, it must have been a bug in the software or something.

kashmir hill

[LAUGHS] Why did you do that? It totally made me think that —

hoan ton-that

Hey, maybe it doesn't work. You never know, right? This could be the long con.

kashmir hill

Ah, O.K.

hoan ton-that

I'm kidding, I'm kidding. It works.

annie brown

What do you think that was about?

kashmir hill

[LAUGHS] I don't think it was a software bug.

hoan ton-that

It's a bug. I don't know. I —

kashmir hill

You have no idea, huh?

annie brown

Huh.

kashmir hill

Yeah. So he said the software bug is now fixed.

hoan ton-that

Oh yes, so I'll show you. This is the iPhone version.

kashmir hill

And he took a photo of me.

hoan ton-that

Oh, it does work.

kashmir hill

Oh, that's so surprising.

hoan ton-that

I know.

kashmir hill

And there, the results included a bunch of photos of me online.

kashmir hill

Oh my god, I totally forgot.

hoan ton-that

Well, we can take —

kashmir hill

That's 10 years ago.

kashmir hill

Including some I had never seen before.

kashmir hill

Some of these photos I didn't know were online.

annie brown

So he's just brushing off this weird thing that happened to you. But do you get the sense that he's thinking at all about privacy?

kashmir hill

So I asked him, you know, this is a very powerful app. And I asked him what restrictions is he thinking about for it. And he said, one, that they were only selling it to law enforcement right now, though it does turn out that they're also selling it to a few private companies for security purposes. But he said they wouldn't sell it to bad actors or bad governments.

hoan ton-that

— and our philosophy is basically, if it's a U.S. based — or like a democracy or an ally of the U.S. — we will consider it. But like, no China, no Russia or anything that wouldn't be good. So if it's a country where it's just governed terribly or whatever, I don't know if we'd feel comfortable selling to certain countries.

annie brown

So it doesn't sound like he has much of a rubric for deciding who to sell to. And it sounds like there's no one really overseeing how he's making these decisions.

kashmir hill

At this point, it's just up to Clearview to decide who they want to sell the app to.

hoan ton-that

No pressure, but when we talk to some venture capitalists, they're like, "Why don't you make this consumer? Law enforcement is such a small market. You won't make that much money." And we've considered it, and we're just like, what's the use case here? And right now, we catch, help catch pedophiles. What if a pedophile got access to this, goes around the street, runs —

kashmir hill

But when I was talking to one of their investors, he says, we want to dominate the law enforcement market, and then we want to move into other markets like hospitality, like real estate. And he predicted that one day, all consumers will have access to this app.

hoan ton-that

Um, and —

kashmir hill

I can tell you that one of your investors hopes that you guys are going to go into the consumer market.

hoan ton-that

Well, yeah. He talks too much. But like, we're not — we're not going to do that. I just don't —

annie brown

Hoan seems to be saying, yeah, there's pressure on us to sell to private consumers, but we're not going to do that. And how reasonable is it to think that he has control or the company has control at this point over where this technology goes?

kashmir hill

I mean, one point that I made when I was talking to him is that oftentimes, the tools that law enforcement use end up in the hands of the public.

kashmir hill

I just — I personally feel like you guys have opened the door to now this becoming more normalized, just because a lot of tools that law enforcement have eventually make their way into public hands.

hoan ton-that

Not always. Not everyone has a gun. [LAUGHS] Right? That would be —

kashmir hill

Anyone who wants one can get one in the U.S. basically, but —

kashmir hill

His response was strange. He said, well, look at guns. Law enforcement has guns, but not everybody has a gun. And I don't know if that's because he's from Australia?

annie brown

Yeah, he's proving your point, in a way.

kashmir hill

[LAUGHS] It did seem like he was proving my point, rather than rebutting it.

[music]

We've been building the technology to make this possible for years now. Facebook building this huge database of our photos with our names attached to it, advances in image recognition and search technologies, it all led us here. But there's been no accompanying regulation or rules around how the technology should be used. There's no real law or regulation that makes this illegal. The scraping seems to be O.K. We don't have a big ban on facial recognition. We don't need to give consent for people to process our faces. And so in terms of holding this tool back, we're just relying on the moral compasses of the companies that are making this technology and on the thoughtfulness of people like Hoan Tan-That.

kashmir hill

But yeah, what do you think about that? Do you think that this is too dangerous a tool for everybody to have?

hoan ton-that

I have to think about that and really get back to you on an answer, because it's a good question.

kashmir hill

Yeah.

hoan ton-that

I've thought about it a little bit.

kashmir hill

You haven't thought about it? You have?

hoan ton-that

I have, I have. But I need to really come up with a good answer for that. Honestly like, yeah.

[music]

annie brown

Thanks, Kashmir.

kashmir hill

Thank you.

michael barbaro

Since Kashmir began reporting on Clearview AI, several major social media companies including Facebook, Twitter and Venmo have demanded that the company stop using photos scraped from their websites. But it's unclear what, if any, power those social media companies have to force Clearview to comply. A few weeks ago, the state of New Jersey barred law enforcement from using Clearview's technology, but police remain free to do so in 49 other states.

We'll be right back.

Here's what else you need to know today. President Trump has begun a campaign of retribution against witnesses in the impeachment inquiry, firing Gordon Sondland, his ambassador to the European Union, who called the president's actions toward Ukraine a quid pro quo. And Lieutenant Colonel Alexander Vindman, a member of the National Security Council, who expressed alarm over the president's phone call with the leader of Ukraine. The Times reports that several Republican senators urged Trump not to fire the witnesses, fearing it would send a dangerous message, but that the president ignored their advice. And the global death toll from the coronavirus has reached more than 800, surpassing that of the SARS epidemic, which killed 774 in 2003. The number of confirmed infections from the coronavirus now stands at more than 37,000. Finally, new polling in New Hampshire, which will hold its primary tomorrow, shows Mayor Pete Buttigieg neck-and-neck with Senator Bernie Sanders and former Vice President Joe Biden slipping into fourth place.

archived recording (george stephanopoulos)

Vice President Biden, the first question is for you. In the last few days, you've been saying that Democrats will be taking too big a risk if they nominate Senator Sanders or Mayor Buttigieg, but they came out on top in Iowa. What risks did the Iowa Democrats miss?

michael barbaro

> The poll, conducted by The Boston Globe, WBZ and Suffolk University suggest Buttigieg is benefiting from a strong performance in the Iowa caucuses and that Biden may perform poorly for the second time in a row, a prediction Biden confirmed during Friday night's debate on ABC.

archived recording (joe biden)

> *Oh, they didn't miss anything. This is a long race. I took a hit in Iowa, and I'll probably take it here.*

michael barbaro

> That's it for "The Daily." I'm Michael Barbaro. See you tomorrow.

Detective Sgt. Nick Ferrara in Gainesville, Fla., said he had used Clearview's app to identify dozens of suspects.Charlotte Kesl for The New York Times

In Gainesville, Fla., Detective Sgt. Nick Ferrara heard about Clearview last summer when it advertised on CrimeDex, a list-serv for investigators who specialize in financial crimes. He said he had previously relied solely on a state-provided facial recognition tool, FACES, which draws from more than 30 million Florida mug shots and Department of Motor Vehicle photos.

Sergeant Ferrara found Clearview's app superior, he said. Its nationwide database of images is much larger, and unlike FACES, Clearview's algorithm doesn't require photos of people looking straight at the camera.

"With Clearview, you can use photos that aren't perfect," Sergeant Ferrara said. "A person can be wearing a hat or glasses, or it can be a profile shot or partial view of their face."

He uploaded his own photo to the system, and it brought up his Venmo page. He ran photos from old, dead-end cases and identified more than 30 suspects. In September, the Gainesville Police Department paid $10,000 for an annual Clearview license.

Federal law enforcement, including the F.B.I. and the Department of Homeland Security, are trying it, as are Canadian law enforcement

authorities, according to the company and government officials.

Despite its growing popularity, Clearview avoided public mention until the end of 2019, when Florida prosecutors charged a woman with grand theft after two grills and a vacuum were stolen from an Ace Hardware store in Clermont. She was identified when the police ran a still from a surveillance video through Clearview, which led them to her Facebook page. A tattoo visible in the surveillance video and Facebook photos confirmed her identity, according to an affidavit in the case.

'We're All Screwed'

Mr. Ton-That said the tool does not always work. Most of the photos in Clearview's database are taken at eye level. Much of the material that the police upload is from surveillance cameras mounted on ceilings or high on walls.

"They put surveillance cameras too high," Mr. Ton-That lamented. "The angle is wrong for good face recognition."

Despite that, the company said, its tool finds matches up to 75 percent of the time. But it is unclear how often the tool delivers false matches, because it has not been tested by an independent party such as the National Institute of Standards and Technology, a federal agency that rates the performance of facial recognition algorithms.

"We have no data to suggest this tool is accurate," said Clare Garvie, a researcher at Georgetown University's Center on Privacy and Technology, who has studied the government's use of facial recognition. "The larger the database, the larger the risk of misidentification because of the doppelgänger effect. They're talking about a massive database of random people they've found on the internet."

But current and former law enforcement officials say the app is effective.

“For us, the testing was whether it worked or not,” said Mr. Cohen, the former Indiana State Police captain.

One reason that Clearview is catching on is that its service is unique. That’s because Facebook and other social media sites prohibit people from scraping users’ images — Clearview is violating the sites’ terms of service.

“A lot of people are doing it,” Mr. Ton-That shrugged. “Facebook knows.”

Jay Nancarrow, a Facebook spokesman, said the company was reviewing the situation with Clearview and “will take appropriate action if we find they are violating our rules.”

Mr. Thiel, the Clearview investor, sits on Facebook’s board. Mr. Nancarrow declined to comment on Mr. Thiel's personal investments.

Some law enforcement officials said they didn’t realize the photos they uploaded were being sent to and stored on Clearview’s servers. Clearview tries to pre-empt concerns with an F.A.Q. document given to would-be clients that says its customer-support employees won’t look at the photos that the police upload.

Clearview’s marketing materials, obtained through a public-records request in Atlanta.

Clearview also hired Paul D. Clement, a United States solicitor general under President George W. Bush, to assuage concerns about the app’s legality.

In an August memo that Clearview provided to potential customers, including the Atlanta Police Department and the Pinellas County Sheriff’s Office in Florida, Mr. Clement said law enforcement agencies “do not violate the federal Constitution or relevant existing state biometric and privacy laws when using Clearview for its intended purpose.”

Mr. Clement, now a partner at Kirkland & Ellis, wrote that the authorities don’t have to tell defendants that they were identified via Clearview, as long

as it isn't the sole basis for getting a warrant to arrest them. Mr. Clement did not respond to multiple requests for comment.

The memo appeared to be effective; the Atlanta police and Pinellas County Sheriff's Office soon started using Clearview.

Because the police upload photos of people they're trying to identify, Clearview possesses a growing database of individuals who have attracted attention from law enforcement. The company also has the ability to manipulate the results that the police see. After the company realized I was asking officers to run my photo through the app, my face was flagged by Clearview's systems and for a while showed no matches. When asked about this, Mr. Ton-That laughed and called it a "software bug."

"It's creepy what they're doing, but there will be many more of these companies. There is no monopoly on math," said Al Gidari, a privacy professor at Stanford Law School. "Absent a very strong federal privacy law, we're all screwed."

Mr. Ton-That said his company used only publicly available images. If you change a privacy setting in Facebook so that search engines can't link to your profile, your Facebook photos won't be included in the database, he said.

But if your profile has already been scraped, it is too late. The company keeps all the images it has scraped even if they are later deleted or taken down, though Mr. Ton-That said the company was working on a tool that would let people request that images be removed if they had been taken down from the website of origin.

Woodrow Hartzog, a professor of law and computer science at Northeastern University in Boston, sees Clearview as the latest proof that facial recognition should be banned in the United States.

“We’ve relied on industry efforts to self-police and not embrace such a risky technology, but now those dams are breaking because there is so much money on the table,” Mr. Hartzog said. “I don’t see a future where we harness the benefits of face recognition technology without the crippling abuse of the surveillance that comes with it. The only way to stop it is to ban it.”

Where Everybody Knows Your Name

During a recent interview at Clearview’s offices in a WeWork location in Manhattan’s Chelsea neighborhood, Mr. Ton-That demonstrated the app on himself. He took a selfie and uploaded it. The app pulled up 23 photos of him. In one, he is shirtless and lighting a cigarette while covered in what looks like blood.

Mr. Ton-That then took my photo with the app. The “software bug” had been fixed, and now my photo returned numerous results, dating back a decade, including photos of myself that I had never seen before. When I used my hand to cover my nose and the bottom of my face, the app still returned seven correct matches for me.

Police officers and Clearview’s investors predict that its app will eventually be available to the public.

Mr. Ton-That said he was reluctant. “There’s always going to be a community of bad people who will misuse it,” he said.

Even if Clearview doesn’t make its app publicly available, a copycat company might, now that the taboo is broken. Searching someone by face could become as easy as Googling a name. Strangers would be able to listen in on sensitive conversations, take photos of the participants and know personal secrets. Someone walking down the street would be immediately identifiable — and his or her home address would be only a few clicks away. It would herald the end of public anonymity.

Asked about the implications of bringing such a power into the world, Mr. Ton-That seemed taken aback.

“I have to think about that,” he said. “Our belief is that this is the best use of the technology.”

Jennifer Valentino-DeVries, Gabriel J.X. Dance and Aaron Krolik contributed reporting. Kitty Bennett contributed research.