Click to prove you're human

The ICO says that, globally, the company has stored more than 20 billion facial images.Clearview AI takes publicly posted pictures from Facebook, Instagram and other sources, usually without the knowledge of the platform or any permission.John Edwards, UK information commissioner, said: "The company not only enables identification of those people, but effectively monitors their behaviour and offers it as a commercial service. That is unacceptable."Mr Edwards continued: "People expect that their personal information will be respected, regardless of where in the world their data is being used."The ICO said Clearview AI Inc no longer offered its services to UK organisations but, because the company had customers in other countries, it was still using personal data of UK residents.In November 2021, the ICO said the company was facing a fine of up to 17m - almost 10m more than it has now ordered it to pay.The UK has become the fourth country to take enforcement action against the firm, following France, Italy and Australia.Lawyer from American firm Jenner and Block, Lee Wolosky said: "While we appreciate the ICO's desire to reduce their monetary penalty on Clearview AI, we nevertheless stand by our position that the decision to impose any fine is incorrect as a matter of law. "Clearview AI is not subject to the ICO's jurisdiction, and Clearview AI does no business in the UK at this time."Clearview AI is advancing public safety by helping law enforcement to rapidly generate leads to identify suspects, witnesses, and victims allowing them to close cases faster and keep communities safe. Clearview AIs highly accurate facial recognition platform is protecting our families, making our communities more secure and strengthening our national security and defense.Clearview AIs highly accurate facial recognition platform is protecting our families, making our communities more secure and strengthening our national security and defense. We help law enforcement and governments in disrupting and solving crime, while also providing financial institutions, transportation, and other commercial enterprises to verify identities, prevent financial fraud, and combat identity theft.We deliver identity intelligence solutions that are:Leading facial recognition technology, excelling even in challenging photographic conditions, tested by NIST.Trained on the largest and most diverse dataset and relied on by law enforcement in high-stakes scenarios. Scalable pricing for agencies and organizations to effectively enable and support their missions.U.S.-based development with the highest certification for data security and cybersecurity policies and procedures.Law EnforcementGovernmentBankingTransportationPaymentsVisitor ManagementSecurityAuthentication Clearview AI is a privately-owned, U.S. based company, dedicated to innovating and providing the most cutting-edge technology to law enforcement, government agencies and the military to investigate crimes, enhance public safety, secure our communities and provide justice to victims. We have developed a revolutionary, web-based intelligence platform for government agencies to use as a tool to help generate high-quality investigative leads. Our platform, powered by facial recognition technology, includes the largest known database of 60+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources.Our solutions empower agencies to gain intelligence, disrupt crime, and enhance public safety by revealing leads, insights and relationships, aiding investigators in solving both simple and complex crimes, ultimately enhancing officer and public safety, and ensuring the safety of our communities and families.James Clayton & Ben DericoBBC News, San FranciscoSpencer Whalen / EyeEmFacial recognition firm Clearview has run nearly a million searches for US police, its founder has told the BBC.CEO Hoan Ton-That also revealed Clearview now has 30bn images scraped from platforms such as Facebook, taken without users' permissions.The company has been repeatedly fined millions of dollars in Europe and Australia for breaches of privacy.Critics argue that the police's use of Clearview puts everyone into a "perpetual police line-up"."Whenever they have a photo of a suspect, they will compare it to your face," says Matthew Guariglia from the Electronic Frontier Foundation says. "It's far too invasive."The figure of a million searches comes from Clearview and has not been confirmed by police. But in a rare admission, Miami Police has confirmed to the BBC it uses this software for every type of crime.Clearview's system allows a law enforcement customer to upload a photo of a face and find matches in a database of billions of images it has collected. It then provides links to where matching images appear online. It is considered one of the most powerful and accurate facial recognition companies in the world. Hoan Ton-That, founder and CEO of Clearview AI, speaking with the BBCThe company is banned from selling its services to most US companies, after the American Civil Liberties Union (ACLU) took Clearview AI to court in Illinois for breaking privacy law. But there is an exemption for police, and Mr Ton-That says his software is used by hundreds of police forces across the US.Police in the US do not routinely reveal whether they use the software, and it is banned in several US cities including Portland, San Francisco and Seattle.The use of facial recognition by the police is often sold to the public as only being used for serious or violent crimes.In a rare interview with law enforcement about the effectiveness of Clearview, Miami Police said they used the software for every type of crime, from murders to shoplifting.Assistant Chief of Police Armando Aguilar said his team used the system about 450 times a year, and that it had helped solve several murders.However, critics say there are almost no laws around the use of facial recognition by police.Assistant Chief of Miami Police, Armando AguilarMr Aguilar says Miami police treats facial recognition like a tip. "We don't make an arrest because an algorithm tells us to," he says. "We either put that name in a photographic line-up or we go about solving the case through traditional means." Mistaken identity There are a handful of documented cases of mistaken identity using facial recognition by the police. However, the lack of data and transparency around police use means the true figure is likely far higher.Mr Ton-That says he is not aware of any cases of mistaken identity using Clearview. He accepts police have made wrongful arrests using facial recognition technology, but attributes those to "poor policing".Clearview often points to research that shows it has a near 100% accuracy rate. But these figures are often based on mugshots. In reality, the accuracy of Clearview depends on the quality of the image that is fed into it - something Mr Ton-That accepts.Civil rights campaigners want police forces that use Clearview to openly say when it is used - and for its accuracy to be openly tested in court. They want the algorithm scrutinised by independent experts, and are sceptical of the company's claims.Kaitlin Jackson is a criminal defence lawyer based in New York who campaigns against the police's use of facial recognition."I think the truth is that the idea that this is incredibly accurate is wishful thinking," she says. "There is no way to know that when you're using images in the wild like screengrabs from CCTV." Kaitlin Jackson, a New York defence lawyerHowever, Mr Ton-That told the BBC he does not want to testify in court to its accuracy. "We don't really want to be in court testifying about the accuracy of the algorithm because the investigators, they're using other methods to also verify it," he says. Mr Ton-That says he has recently given Clearview's system to defence lawyers in specific cases. He believes that both prosecutors and defenders should have the same access to the technology. Last year, Andrew Conlyn from Fort Myers, Florida, had charges against him dropped after Clearview was used to find a crucial witness. Mr Conlyn was the passenger in a friend's car in March 2017 when it crashed into palm trees at high speed.The driver was ejected from the car and killed. A passer-by pulled Mr Conlyn from the wreckage, but left without making a statement. Although Mr Conlyn said he was the passenger, police suspected he had been driving and he he was charged with vehicular homicide.His lawyers had an image of the passer-by from police body cam footage. Just before his trial, Mr Ton-That allowed Clearview to be used in the case."This AI popped him up in like, three to five seconds," Mr Conlyn's defence lawyer, Christopher O'Brien, told the BBC. "It was phenomenal."Andrew ConlynThe witness, Vince Ramirez, made a statement that he had taken Mr Conlyn out of the passenger's seat. Shortly after, the charges were dropped. But even though there have been cases where Clearview is proven to have worked, some believe it comes at too high a price. "Clearview is a private company that is making face prints of people based on their photos online without their consent," says Mr Guariglia."It's a huge problem for civil liberties and civil rights, and it absolutely needs to be banned."Viewers in the UK can watch the Our World documentary into Clearview AI on BBC iPlayer While Clearview AI has finally settled some of the legal cases against it, the U.S. facial recognition company remains in danger of penalties and legal actions on both sides of the Atlantic.On Monday, the UKs data privacy watchdog called for the reinstatement of a 7.5 million pounds (US$10 million) fine against the company, arguing that the judges who overturned it in 2023 made errors in their decision. The appeal case, which was heard at the Upper Tribunal in London, marks yet another turn for the drawn-out dispute. The countrys Information Commissioners Office (ICO) issued an enforcement notice to the firm in May 2022, requiring Clearview to delete the personal data of UK individuals collected through facial recognition technology, along with a fine for alleged UK General Data Protection Regulation (GDPR) violations. The following year, however, the company successfully appealed the enforcement action.At the time, Clearview argued that its clients are exclusively foreign government bodies or their contractors exercising criminal law enforcement and national security functions, which are out of the UKs legal scope. The UKs First-Tier Tribunal agreed with the firm.That decision is now being challenged by the ICO with the help of Privacy International, which was permitted by the court to intervene in the proceedings, according to MLex.The data protection authority says that the lower court decision failed to distinguish between Clearviews clients that were foreign states and those that were private contractors working for foreign states or their law enforcement bodies. In this way, the First-Tier Tribunal illegitimately extended the immunity that foreign states have against the UK GDPR to private sector entities, according to ICOs solicitor, Timothy Pitt-Payne.Clearview AIs defense, on the other hand, argues that only 20 percent of its clients are private contractors.The company is facing other penalties in Europe, including one levied by the Italian data protection regulator for violating the EUs GDPR.In April, Data Protection Authority Commissioner Guido Scorza said that he has been working with U.S. authorities to notify Clearview of its enforcement action and the 20 million euro (US$22.8 million) fine levied in 2022. The fine is currently unpaid while Italian citizens data remains on Clearviews servers despite orders to delete it.Clearview in danger of more lawsuits in the USClearview is also still facing scrutiny on its home turf.In May, the company officially settled a five-year-long biometric data privacy lawsuit against it after multiple consolidation orders and rounds of mediation. The nationwide class settlement awarded a payout to the plaintiffs from a 23 percent equity stake in Clearview, which will be triggered by an IPO or a liquidation event such as a sale or bankruptcy.As of January 2024, Clearviews value was estimated to be approximately $225 million, making the settlement worth $51.75 million.But not everyone is happy with the result, according to a legal analysis of the case by the Troutman Pepper Locke law firm. The U.S. state of Vermont, for instance, filed its own lawsuit in April, which could ban Clearview AI from operating within that state if successful.More states that follow suit, create greater jeopardy for Clearview AIs business model for jeopardizing the potential monetary relief of the class, says Daniel Waltz, one of the law firms associates.The May settlement was approved over the objection of attorneys general from 22 states and the District of Columbia. They argued that the deal does not guarantee that consumers who filed the lawsuit will get monetary compensation. If Clearview AIs worth drops, the plaintiffs may end up with nothing.Another concern is the lack of a meaningful injunctive relief, meaning that the company was not ordered to stop doing something harmful or illegal nor was it forced to take a specific action to repair harm.I just think that this settlement really does provide precedent for creative settlement negotiations and terms, says Lauren Geiser, another associate at Troutman Pepper Locke. I know the AGs obviously are not a fan of the 23 percent because it could be nothing for the class, but it could also be very lucrative to the class, depending on how this unfolds and how Clearview performs. Article Topics biometric data | biometrics | Clearview AI | facial recognition | Information Commissioners Office (ICO) | lawsuits | United States Demand for biometrics in established applications like national ID programs and border control is strong, as seen in several of A common complaint from opponents of age assurance technology is that parents should be the ones to decide what their The Chairman of the Papua New Guinea (PNG) National Research Institute, Wilson Thompson, has made the case for a revalorization Hopae has won major backing as it collaborates on a joint research institute with the South Korean government in building Only 35 percent of adult Germans have activated their electronic identity, despite the country offering eID functionality since 2010, according The OpenID Foundation has successfully completed an interoperability test of its OpenID for Verifiable Credential Issuance (OpenID4VCI) specification, which allowed Today, Im talking to Kashmir Hill, a New York Times reporter whose new book, Your Face Belongs to Us: A Secretive Startups Quest to End Privacy as We Know It, chronicles the story of Clearview AI, a company thats built some of the most sophisticated facial recognition and search technology thats ever existed. As Kashmir reports, you simply plug a photo of someone into Clearviews app, and it will find every photo of that person thats ever been posted on the internet. Its breathtaking and scary.Kashmir is a terrific reporter. At The Verge, we have been jealous of her work across Forbes, Gizmodo, and now, the Times for years. Shes long been focused on covering privacy on the internet, which she is first to describe as the dystopia beat because the amount of tracking that occurs all over our networks every day is almost impossible to fully understand or reckon with. But people get it when the systems start tracking faces when that last bit of anonymity goes away. And its remarkable that Big Tech companies like Google and Facebook have had the ability to track faces like this for years, but they havent really done anything with it. It seems like thats a line thats too hard for a lot of people to cross.Listen to Decoder, a show hosted by The Verges Nilay Patel about big ideas and other problems. Subscribe here!But not everyone. Your Face Belongs to Us is the story of Clearview AI, a secretive startup that, until January 2020, was virtually unknown to the public, despite selling this state-of-art facial recognition system to cops and corporations. The companys co-founders Hoan Ton-That and Richard Schwartz are some of the most interesting and complex characters in tech with some direct connections to right-wing money and politics.Clearview scraped the public internet from billions of photos, using everything from Venmo transactions to Flickr posts. With that data, it built a comprehensive database of faces and made it searchable. Clearview sees itself as the Google of facial recognition, reorganizing the internet by face searches and its primary customers have become police departments and now the Department of Homeland Security.Kashmir was the journalist who broke the first story about Clearviews existence, starting with a bombshell investigation report that blew the doors open on the companys clandestine operations. Over the past few years, shes been relentlessly reporting on Clearviews growth, the privacy implications of facial recognition technology, and all of the cautionary tales that inevitably popped up, from wrongful arrests to billionaires using the technology for personal vendettas. The book is fantastic. If youre a Decoder listener, youre going to love it, and I highly recommend it.Our conversation here hits on a lot of big-picture ideas: Whether we as a society are just too nihilistic about privacy to make the difficult but necessary tradeoffs to regulate facial recognition; what kinds of policy and legal ideas we even need to protect our privacy and our faces; and what aws are even on the books right now. Theres an Illinois biometric privacy law that comes up quite a bit in this conversation and at the end Kashmir tells us why shes actually hopeful why were not going to live in a dystopian future. Its a great conversation, its a great book. I loved it, I think youre really going to like it.Here is Kashmir Hill, author of Your Face Belongs to Us. Here we go.Kashmir Hill, you are the author of Your Face Belongs to Us, a book about a startup called Clearview AI, and youre also a tech reporter at The New York Times. Welcome to Decoder.I am really excited to talk to you. I have followed your work for years and years. You have been on what some might call the privacy beat, what you call the dystopia beat. Theres a deep relationship between those ideas in the context of technology, and it all comes to a head in this book, which is about a startup called Clearview. It is founded by a number of characters. There are a number of links to the alt-right, the whole thing. But fundamentally, what they do is scan faces and do facial recognition at scale, and there are just a lot of themes that collide in this book. It is kind of an adventure story. Its a lot of fun. Lets start at the very beginning. Describe Clearview AI and what they do and why they do it.Clearview AI basically scraped billions of photos from the public internet. They now have 30 billion faces in their database collected from social media sites like Facebook, Instagram, LinkedIn, Venmo. They say that their app identifies people with something like 98.6 percent accuracy. And at the time I found out about them, they were secretly selling this kind of superpower to police, and no one knew about it.That first step, were going to take a bunch of faces off the public internet a lot of technology companies start by just taking stuff off the public internet. We are in a time right now that the context of everything is generative AI. There are a million lawsuits about whether you should be able to just freely scrape information off the public internet to train a generative AI system. That theme comes up over and over again, but theres something in particular about faces and what Clearview AI did with faces that everyone reacts differently to. Why do you think that is?I just think its so personal. Who we are is in our face. And this idea that anyone can snap a photo of us and suddenly know not just who we are and where we live and who our friends are, but dig up all these photos of us on the internet going back years and years. I think theres just something inherently privacy-invasive about that that just is more resonant for people than cookies or tracking what websites youve been to. Its really controlling your identity.As youve been talking about the book, promoting the book, have you sensed that people respond to it differently when its faces? The reason I ask this is because you have done a lot of reporting about cookies, about advertising tracking, about all of these pretty invasive technologies that permeate the internet and, thus, modern life. It always feels pretty abstract. You have to start by explaining a lot of stuff to get to the problem when youre talking about cookies on a website or advertising or something. When you start with faces, it seems immediately less abstract. Have people responded to the book or the ideas in it differently because its faces?Well, one, just everyone gets the face, right? You dont need to be a technology expert to understand why it might be invasive for somebody just to know who you are or find your face in places that you dont want them to find it. I also think that it builds on all that privacy reporting Ive been doing for years all that online tracking, all those dossiers that have been created about us online, that weve created and that other people have created on us.The face is the key to accessing all that in the real world. All this online activity, the dossier, can now just be attached to your face as youre moving, as youre walking down the street, when youre making a sensitive purchase at a pharmacy, when youre trying to get into Madison Square Garden. All of a sudden, its like your Google footprint attached to your face.Talk about Clearview AI itself, because the big companies have kind of had this capability for a while, and to their credit, they havent really done much with it. Google, inside of Google Photos, will do some face matching, but thats not public as far as we know. Facebook can obviously do it, but they keep that inside of Facebook. Clearview is just like, Were doing it. We took a bunch of data, and were doing it. Now the cops can look at your face. Why is this company different? How did it start?I think this was really surprising to people its something thats in the book that Google and Facebook both developed this ability internally and decided not to release it. And these are not companies that are traditionally that conservative when it comes to private information. Google is the company that sent cars all over the world to put pictures of our homes on the internet.What was different about Clearview AI is that they were a startup with nothing to lose and everything to gain by doing something radical, doing something that other companies werent willing to do. I put them in the same category of being a regulatory entrepreneur as an Uber or an Airbnb that this was their differentiator. They said, Were going to make this database, and were going to reorganize the internet by face, and thats our competitive advantage. And we want to make our database as big as we can before anyone else can catch up to us.Were they searching out the market of police departments and right-wing influencers, or did they start with that political bent from the beginning? Because thats a real theme of your book, that a bunch of characters are floating around this company from the start that are not necessarily great characters to be under a company, but they seem to have welcomed it.Yeah, so Clearview AI is really a strikingly small company, just a ragtag group of people, I think exemplified by the technical co-founder, Hoan Ton-That. This young guy, he grew up in Australia, obsessed with technology, obsessed with computers. [At] 19 years old, drops out of college and moves to San Francisco, and hes just trying to make it in the tech gold rush. It was 2007. He becomes a Facebook developer, then he starts doing these silly iPhone games. And he makes an app called Trump Hair where you can put Donald Trumps hair on people in your photos. Just throwing spaghetti at the wall to see what will stick. And he starts out kind of liberal. He moves to San Francisco, grows his hair long, plays guitar, hangs out with artists. And then he moves Yeah. [Laughs] And then he moves to New York and really falls in with this conservative group of individuals. People had a lot of far-right interests. And [he] was able to build this radical technology because its open source now; its very accessible. Anyone with technical savvy and the money to store and collect these images can make something like this. And they were able to have money around them. He met Peter Thiel at the Republican National Convention, and Peter Thiel ends up becoming the first investor in the company that became Clearview AI, giving them $200,000. Though they eventually ended up selling it to police departments, originally, it was just searching. It was a product in search of a user, and they had all kinds of wild ideas about who might buy it.Those ideas are really interesting to me. I can see a lot of ways that a consumer might want to search the internet by face, or retail stores, like you mentioned. You walk into a store, they want to know who you are, what youve bought before. There are a lot of markets. And somehow, theyve ended up with the authorities, which is maybe the last market anybody wants. How did they end up with the cops?So, they originally were trying to sell it to private businesses: hotels, grocery stores, commercial real estate buildings. They would also give it to investors and people who own those grocery stores and buildings. Thats one of my favorite anecdotes about one of the first users of Clearview AI: this billionaire in New York, John Catsimatidis, who had the app on his phone, was thinking about putting it in his grocery stores to identify shoplifters, specifically Hagen-Dazs thieves, and ends up in an Italian restaurant in SoHo. His daughter walks in, and shes got a man on her arm, and he didnt know who it was, so he asked a waiter to go over and take a photo of them and then runs the guys photo through Clearview AI and figures out who he is. Hes a San Francisco venture capitalist, and he approved.But yeah, originally, they were just like, Who will pay for this? When it was getting vetted at one of these real estate buildings as a tool to use in the lobby to vet people coming in, the security director loved it and said, You know who would really benefit from this? My old colleagues at the NYPD. And so thats how they got introduced to the New York Police Department. NYPD loved it, and lots of officers there started secretly using it. This shocked me that police can just essentially get this unvetted tool from some random company and download it to their phones and just start using it in active investigations. But thats what happened. And Clearview gave them free trials. They told their friends, other departments. All of a sudden, the Department of Homeland Security is getting access to it and officers around the world. And everyones just really excited to have this new, very powerful tool that searches the whole internet looking for somebody.Theres a big assumption baked in there. Youve hit on it. Its unvetted. Youve used it, youve had it used on you. Does it work?So I have never had access to Clearview AI myself. Ive asked many times, Hey, can I download the tool? And they say its only for police departments, now at least. But Hoan Ton-That has run searches on me several times. I talked to him a lot for the book. For me, it was very powerful. It turned up 160 or so photos of me, from professional headshots that I knew about to photos I didnt realize were online. A photo of me with a source Id been talking to for a story. I remember this one photo of somebody, and theres a person walking by in the background. And when I first looked, I didnt see me. Then I recognized the coat of the person in profile walking by in the background. Its a coat I bought in Tokyo, very distinctive. And I was like, Wow, thats me. I couldnt even recognize myself. Ive seen searches that law enforcement has done. It really is quite powerful. I think facial recognition technology has advanced in ways that most people dont realize.And is it powerful at the average level of facial recognition technology? Is Clearview more powerful than the average piece of technology? Where does it land on that scale?At the time that I first heard about them and in the first few years working for law enforcement, they hadnt been vetted. No one had tested their algorithm for accuracy in a rigorous way but there is a federal lab called NIST, or the National Institute of Standards and Technology, and they run something called the [Face Recognition Technology Evaluation.] And so theyll test all these algorithms. And Clearview, the first time they did the test, they came out really high on the scale. They actually do have quite a powerful algorithm that was really one of the best in the world. And I think, at the time, it was the top-rated algorithm from an American company. So, they do have a good algorithm.And you said its open source, and its a ragtag team. How are they outdoing everyone else? Whats the secret to their success here?Its not completely open source. Hoan Ton-That was not a biometric kind of genius. He didnt have any experience specifically with facial recognition technology. His introduction to it was through academic papers and research that was being shared online. But he did recruit someone who had some more experience with machine learning and neural net technology. And he said they fine-tuned the algorithm. They trained it on lots of faces collected from the internet. So clearly, theyre doing something right there. But it started with... I mean, he started from zero. He went from Trump Hair to this radical app with 30 billion faces. Its quite a story.That database of faces is really interesting to me because it doesnt belong to them. Theyve scraped it from social media sites. Theyve scraped it from the public internet. Theyre looking for photos of you; they find them. They clearly have not taken those photos of you. Someone else has taken those photos of you. How is it that they remain in possession of this dataset now that the company is public and everyone knows that they scraped all of this information?Several years ago, some of the companies whose data they had scraped, whose users data they had scraped Facebook, Google, Venmo, LinkedIn sent Clearview cease-and Venmo was actually one of the very first sites they scraped, which was interesting to me because Venmo has gotten a lot of scrutiny from privacy activists who said that it was very bad for users that Venmo makes everybody public by default that all your transactions are public by default unless you change your privacy settings. Privacy activists have been criticizing them for years and years and years. And Hoan told me, Yeah, that was great for me because on the Venmo.com website, they actually were showing real-time transactions, public transactions between users, and it would update every few seconds. It had photos of the users and links to their profile page. And so he developed a scraper that just hit that site every few seconds, and it was like a slot machine where he just pulls it and faces come spilling out. So yeah, Venmo was in there.These companies sent Clearview AI cease-and-desist letters. [They] said, Hey, youre violating our terms of service. Youre not supposed to do this. We see this as a violation of contractual law, the Computer Fraud and Abuse Act. Then, that was it. No one sued Clearview AI. No one forced the company to delete the photos. As far as I know, Clearview AI still has them and is still collecting Why has no one sued them? This is bonkers to me.Ive never really gotten a satisfactory answer to this, honestly. I think part of it is that its a bit of a legal gray area, whether its illegal to scrape or not. And there are a lot of digital rights groups who want us to have the ability to scrape, to make it easier to collect information thats on the public internet. Theres at least one federal court ruling in this case between LinkedIn and HiQ, the startup that was scraping information from LinkedIn to basically let employers know if any of their employees were thinking about leaving. The finding in that case was that scraping was legal. And so I think part of it is that these companies dont think theyd win if they sued. And then, I dont know. Maybe they just dont want to bring more attention to the fact that the horse is already out of the barn, that Clearview already has all of their users photos.Or theyre taking advantage of the gray area, too. Thats the thing that just leaps out to me, is Google is training all of its AI systems on the public internet, and so is Amazon, and so is Facebook, and so is OpenAI. And if you go chase down Clearview AI, you might cut yourself off. But then, on the flip side, theres a bunch of users. Theyre your photos. Theyre our photos. Theyre not the platforms photos. If I upload photos to Facebook, Facebook is very clear like, These are still your photos. Weve signed some license with you, or youve not read a license and clicked I accept, more likely, that says we can use them. But theyre still my photos. Why havent any users gone after Clearview AI?Clearview has been sued in a few states where theres a relevant law. Theres a lawsuit in California. The Vermont attorney general sued them. And basically, a whole bunch of litigation got consolidated in Illinois because Illinois is one of the few states that has this really strong law directly applicable to what Clearview AI did called the Biometric Information Privacy Act, or BIPA. I tell the history of it in the book. Its a bit of a fluke of history that it was passed, but its the rare law that moved faster than the technology. And so, yeah, theyre fighting. Theyre trying to say, Hey, you violated our privacy. You violated this law. Get us out of your databases. The law moves very slowly, as anybody whos ever watched a lawsuit happen [knows], and so those kind of suits have been going on for years now.The thing that really broke this company into the mainstream and made people pay attention to it is your reporting. The cops are using it, people were using it, these characters on the right wing were using it. But the company sought no publicity. It didnt want anyone to be known. And you started reporting on it. They still tried to hide. And then something happened, and Hoan Ton-That started talking to you and honestly started being proud of his company in a very different way, publicly proud of what they were doing. What was the change there? What happened?Yeah, when I first started reporting on Clearview AI, they very much wanted to stay in the shadows. And they actually were not talking to me but tracking me. They put an alert on my face so that when law enforcement officers who I was talking to uploaded a photo of me to show me what the results were like, the company would get an alert, and they would reach out to the officers and tell them, Stop talking to her. They deactivated one of their accounts. That was a bit creepy for me.But, at some point, they changed their mind, and they hired a crisis communications consultant, basically an expert that you go to when youre having a PR disaster. And they went with this woman who... Shes a political person. She was who Eliot Spitzer called when he was having his troubles. And I think she told them, Look, you cant stop her. Shes going to do this story. And we need to go on the offensive here. We need to defend what youve built and try to make sure that your company stays in existence and can keep doing business. Because it looked pretty bad when I first started looking into them. Their efforts to hide themselves while theyre exposing so much about millions of people was not a good look.So when the tone changed and they hired a crisis person, they started engaging with you in the reporting. What was the pitch for why this was a good thing to build? I can come up with hypothetical reasons why some hypothetical facial recognition system is good to build, but here youve got a real one here. Here, youve got actual cops who are using it. Youve got a bunch of downstream obvious bad things that are happening. What was their pitch for why it was good?What Hoan Ton-That says, what hes evolved into around facial recognition technology, is that what the company is selling this power for police officers to identify criminal suspects, to solve crimes is the best possible use of facial recognition technology. That they are making the world safer, more secure. Its being used to rescue children. I remember this line from that first interview I had for him, where he said, Theyre using facial recognition technology to find and arrest pedophiles; its not getting used by pedophiles. And so this is what they really lean into that this is a technology that is making the world safer. And theyre restricting its use to law enforcement, so this is good, that society should embrace this.So this runs right into the tradeoffs of all technology that is used by law enforcement. It seems like they are a battering ram of rhetoric when it comes to why law enforcement is using it. Like you say, Were catching pedophiles, and thus, no more questions should be asked. Whenever I hear that, the red flags go off for me. Youre trying to prevent me from asking questions about the Fourth and Fifth amendments. Youre trying to prevent me from asking questions about privacy by making them seem morally wrong to ask. But theres a part of me that says, Look, the technology definitely has an error rate. I dont know what the cops are doing. I cant audit their use of it. When they do rely on technology like this, history and statistics suggest that they will have a disproportionate impact on marginalized communities. Has Clearview addressed any of this, or are they just saying the classic tech company line of, This is a tool, and tools are neutral and it depends on who uses it and why?Clearview definitely pushes that onus to police departments in saying, Were just providing the technology for them to use. They should never arrest somebody based on a Clearview match alone and that they need to do more investigating. I think, for us as a society, theres just a lot to evaluate here. Ive talked to a lot of officers who, yeah, theyve solved crimes with Clearview AI as a starting point. And horrific things abuse of children. But I think we need to ask ourselves, are we comfortable with this database of probably hundreds of millions of people, probably you and me? Should we all be in the lineup every time the police are trying to solve a crime, whether its shoplifting or murder? And if they are going to use facial recognition technology, what are the rules? Do you need to get a warrant to search a database like this? Should every officer just have this on their phone and use it whenever they want? What do you do after you get a match? What kind of crime should you use it for?Even if we just accept that its a useful tool, there are still so many conversations we have to have. I know of at least one person who has been misidentified as a criminal suspect because of Clearview AI. He lived in Georgia. It was basically purse theft in Louisiana. He was the hit. He got arrested the day after Thanksgiving, put in jail for a week, awaiting extradition. Louisiana had to hire lawyers to clear all this up. It can be really damaging when it goes wrong or if the police trust the face match too much not to mention what happens if it starts getting rolled out more widely. And we look at China as an example of that. What if we start having a technology like this running all the time on all the cameras, tracking us everywhere we go? It could be used in chilling ways against protestors or to gather damning information about a political opponent. Its such a range that I really think we need to think hard about this and not just let it slip in and become ubiquitous or become normalized without setting up some guardrails.So I can already hear the responses from some of our listeners who think you cant put the genie back in the bottle ever, and your privacy is already gone. Just by holding a smartphone, your privacy is already gone. And what is the difference between having your face out there versus your already gigantic digital fingerprint? Is the genie just out of the bottle? It feels like we might be in a liminal moment where there is a law in Illinois, and maybe there should be a federal law. Or maybe we should just say stop in some way. Just scream out the windows, Please stop. But theres a chance that its already over, and a generation of young Americans in particular just believes that all the cameras on the internet, the cops can look at them, and thats going to be that.I am not a privacy nihilist. If I were, I probably wouldnt be on the beat because whats the point?I do think that we can change course, and I do think that we can restrain technologies through norms and through policies and regulations and laws. We could live in a world where there were speed cameras on every road and jaywalking cameras everywhere, and if you sped or if you jaywalked, you would immediately get a ticket. But I dont think any of us want to live in that world. And so, even though thats possible, it doesnt exist. Jay Stanley at the ACLU gave me this great example of a time that weve restricted technology, and thats last century, when there were all these tiny bugs and recording devices that were starting to get manufactured. If youve heard the Nixon White House tapes, then youve benefited from that technology. People at the time were freaking out that they were just going to be recorded all the time, that you could no longer have a private conversation, that there were just these bugs everywhere.And we passed laws to make eavesdropping illegal, to restrain the ability to record conversations. And its the reason why all of these surveillance cameras that just are everywhere in public space now are only recording our images and not our conversations. I dont think we just need to accept that were going to live in this dystopian world because technology makes it possible. I think that we can choose the world that we live in. I hope that we wont just have ubiquitous facial recognition all the time. Because I think it would be so chilling to not be able to gossip at dinner without the worry that a person next to you is going to identify you with an app on their phone and blast out what youre talking about on Twitter, or X, as we call it these days.Put that into practice for me. Ive read a lot of your reporting. A lot of your reporting is about how the Big Tech companies build these ubiquitous surveillance networks, mostly to put advertising in front of us. At the end of it all, theyre just trying to sell us some paper towels, and faster than ever before. And there are billions of dollars in between me and the paper towels. But thats what its for. Its very targeted advertising. And theres some debate about whether its even effective, which I think is very funny, but thats what its largely for. And I go out, I see my family, I listen to our readers, and theyre like, Facebook is listening to us on our iPhones. And they wont believe me that probably not. Thats probably not happening, that theres this other very complicated multibillion-dollar mechanism that just makes it seem like Facebook is listening.It would be very illegal.But theyve just given up, right?Itd be very illegal if they were.It would be illegal, and also it would be harder. It feels like it would be much harder to light up your microphone all the time and listen to you than just assemble the digital fingerprint that theyve managed to assemble and show you the ads for a vacation that your friend was talking about. You can explain it, but then people just fall back on, Well, Facebook is just listening to me on my phone, and I still have a phone and its fine. And thats the nihilism, right? Thats where the nihilism comes into play, where even when people assume that one of the most invasive things that can happen is happening, theyre like, But my phones so useful. I definitely need to keep letting Facebook listen to me.Yeah, Im still going to take it with me to the bathroom.Right. You ask somebody if they would put a camera in the bathroom, and theyre like, No. And youre like, Well, you carry seven of them in there all the time. But of course, you have to have your phone in your bathroom. Do you see that changing at the policy level? Okay, now heres a set of technologies that is even more invasive or can do this tracking that we dont think we should do, or could get a politician into trouble like it did with Nixon, or X, Y, and Z bad thing could happen, we should probably restrict it before it gets widespread. Or is the nihilism, the cultural nihilism around privacy, still the dominant mode?I feel like were at the tipping point right now of deciding, are we going to continue having anonymity in our everyday life, in our public spaces, or not? I hope we go the way of yes, and I feel like lawmakers, oftentimes, it is very private for them and how does this get used against them. I think about that crazy recording from the Beetlejuice show, and youre fondling your boyfriend and getting fondled, and you kind of think youre anonymous.I wasnt sure where that was going to go. I thought you were going to talk about the actual movie Beetlejuice and not Lauren Boebert, but yeah, Im glad we got there.I think thats the first time anyone said fondle on Decoder, I want to be clear.You think youre in a crowd and youre anonymous, and you dont realize they have these night vision cameras at the show staring down at you capturing everything thats happening. I think if we have more moments like that that affect lawmakers where, yeah, they thought they were in this private space. They didnt think that it was being taped, that it would be tied back to them. I just think, all of us, even if you think, Oh, Im fine, Id be fine with people knowing who I am, there are moments in your day where youre doing things that you just wouldnt want easily known by strangers around you, or a company, or government. I just think that that is true.And we have seen this get restricted other places. Like Europe investigated. All the privacy regulators in Europe and Canada and Australia, they looked at what Clearview did, and they said, This breaks our privacy laws. Youre not allowed to collect peoples sensitive information, biometric face print, this way and do what youre doing. And they kicked Clearview AI out of their countries.Is Clearview still collecting the data? Are they still scraping the internet every single day, or is the database fixed?So, when I first wrote about them in January 2020, they had 3 billion faces. And today, they probably have more, but last I heard, they had 30 billion faces. So they are continuing to grow their database.Do we know what the sources are of that growth? Is it still the public internet, or are they signing deals? Hows that working? Unfortunately, theyre not a government actor. Theyre a private company, so I cant send them a public records request and find out what all their sources are. So, I mostly see it through when I see an example of a search, whether they run it on me or I see it show up in a police investigation. But yeah, it seems like pretty wide out there news sites, employer sites. They seem to be pretty good at targeting places that are likely to have faces. And one of my last meetings with Hoan Ton-That, before I was done with the book, they had just crawled Flickr. He himself was finding all these photos of himself when he was a kid, like a baby coder in Australia. He said, Its a time machine. We invented it. And he did a search on me, and it showed photos I didnt know were on Flickr that one of my sisters friends took. It was me at a point in my life when I was depressed, I was heavier, I weighed more. I dont put photos from that time on the internet, but there they were. Clearview had them.We have a joke on The Verge staff that the only functional regulation on the internet is copyright law. If you want something to come down off the internet, your fastest way to doing it is to file a DMCA request. Im shocked that a bunch of Flickr users havent done this with Clearview. Im shocked that someone else has not realized, Okay, this company boosted my photos. Getty Images, we just had the CEO on Decoder, Im shocked that they havent done this. Is it just the company is still in the shadows, or have they actually developed a defense? It just seems, at this point, given the nature of copyright lawsuits on the internet, its out of the norm that there isnt one.Yeah, Im not a lawyer. I just played one when I was a baby blogger at Above the Law.What Clearview often argues is that they are very comparable to Google, and they say, These are not our images. Were not claiming ownership over these images; we are just making it searchable in the same way that Google makes things searchable. And when you do a search in Clearview AI, all it shows you is the little face, and you have to click a link to see where the full image is on the internet and where it came from. I have talked to officers who have found deleted photos with Clearview AI, so it makes me think that they are in fact storing the images. But yeah, I havent seen somebody make that argument against them yet.So its interesting. Someone did once upon a time make that argument against Google, and there is that case. Were already in the Boebert zone, so Ill say it was Perfect 10 v. Google. Perfect 10 was a soft-core porn magazine, I think, and Google was doing Google Images, and they were taking the thumbnails. A lot of the law of the internet is like this. Its the way it is.There is Google Images, there is reverse-image search on Google. Do you see a difference in those two things? Im confident that I could put my face in the Google Image reverse search, and it would spit out some answers that look like me or are me. Is there a meaningful difference here?Clearview AI is, in so many ways, building on the technology that came before it from, yeah... They ended up hiring Floyd Abrams as their lawyer, preeminent First Amendment lawyer, worked for The New York Times to defend the right of the newspaper to publish the Pentagon Papers. And he was specifically talking about precedent from Google cases that supported what Clearview AI was doing. That theyre a search engine, and instead of searching for names, theyre searching for faces. That hasnt been completely successful for them in the courts. Judges have said, Okay, fine. You have the right to search images and look at whats out on the internet, but you dont have the right to create this biometric identifier for people. That that is an extra step too far.But in so many ways, theyre building on what came before from all these technology companies encouraging us to put our photos online, put our faces online next to our names, to the actual technologies and algorithms that engineers at universities and at these companies developed and then made available to them. So yeah, theyre building on what came before. I dont think that necessarily means that we do have to keep letting them do what theyre doing. But so far, we have in the US, in much of the US.So you mentioned the courts. There was a case in Illinois, the ACLU sued Clearview for violating the Illinois biometrics law that you mentioned. They settled, and part of that settlement was Clearview agreeing to only sell the product to law enforcement and no one else. That seems like an awfully gigantic concession: we will have no customers except the cops. How did they get there? How did that affect their business?It was funny because both sides presented the settlement as a win. The ACLU said, We filed the suit because we wanted to prove that this Illinois law, BIPA, works, and Clearview AI did try to say that its unconstitutional, that it was a violation of their First Amendment right to search the internet and access public information. That didnt work. They had to settle.So ACLU said, Hey, we prove that BIPA works. Other states need BIPA. We need BIPA at the federal level. Meanwhile, Clearview agreed in the settlement to restrict the sale of their database only to the government and law enforcement. And so ACLU said, Hey, we won, because now this huge database of billions of faces wont be sold to companies, wont be sold to individuals. But Clearview said, Hey, this is a win for us. Were going to continue doing what were doing: selling our tool to the police.And they do still have lots of contracts with police departments. They have a contract with the Department of Homeland Security, the FBI, widely used by the government. But it was important in that, yeah, it means they cant sell it to private companies. So that cuts off one line of business for them.Does that limit the size of their business? Are their investors happy about this? Are they sad about this? Is Peter Thiel mad that the company isnt going to go public or whatever?So one of the investors that Ive talked to a few times is David Scalzo. He was a venture capitalist out here on the East Coast. He was so excited about investing in Clearview AI because he told me they werent just going to sell this to police they were going to sell this to companies; they were going to sell this to individuals. He said, Everyone in America is going to have the Clearview AI app on their phone. The moms of America are going to use this to protect their children. And he thought he was going to make a ton of money off of Clearview AI. He said, Its going to be the new Google. The way you talk about Googling someone, youre going to talk about Clearviewing their face. And so he has been frustrated by the company agreeing to tie its hands, just selling it to police, because he says, I didnt want to invest in a government contractor. And yeah, there is a question about the future of Clearview.When I think of not lucrative businesses, I think of government contractors.No government contractor has ever made a killing.So yeah, hes not happy about it. And Clearview sell their technology for very cheap compared to other government contractors.Yeah. When I first started looking into them, and Im getting these government contracts showing up in public records requests. In some cases, they were charging police like $2,000 a year for access to the tool. It was like one subscription for $2,000. Now, their most recent one they signed with the Department of Homeland Security, is close to $800,000 for the year. So, either theyve got a lot of users It still seems cheap, right? But either they have a lot of users Take DHS for all theyre worth.Either they have a lot of users, or DHS is like, Were going to pay you a lot because we want to make sure that you stay in business.Yeah, thats the part that Im really curious about. Is there competition here? Is Raytheon trying to build a system like this? If you see a market, particularly a lucrative government contracting market, it seems like the big companies should be racing in to build competitive products or more expensive products or better products. Is that happening, or are they in a market of one?There are copycats. Theres this public face search engine that anyone can use called PimEyes. It doesnt have as large a database. It doesnt have as many photos come up, but it is out there. I havent heard about anyone else doing exactly what Clearview is doing and selling it to police. Most other companies just sell a facial recognition algorithm, and the customer has to supply the database of faces. So that does set Clearview apart.I wonder how its going to affect other businesses, just the reaction to Clearview. It has been such a controversial company. It has run into so many headwinds, and its unclear at this point how expensive this is going to be. Theyve had fines levied by European privacy regulators that they have so far not paid, and this Illinois law is very expensive to break. Its $5,000 per person whose face print you use. It cost Facebook $650 million to settle a lawsuit over BIPA for automatically recognizing faces to tag friends in photos. It could break the company. Clearview has only raised something like $30 million. So yeah, I keep waiting to see whats going to happen financially for them.It would be incredible if the Department of Homeland Security is funding a bunch of fines to the Illinois government to keep this company afloat. But thats the cycle were in. The revenue is going to come from law enforcement agencies to pay fines to a state government instead of there being any sort of federal law or cohesive regulatory system. Is any change there on the horizon that there might be a federal facial recognition law or more states might look at, quite frankly, the revenue that Illinois is going to gain from this and pass their own laws? Or is it still status quo?Its strange to me because I hear so often from lawmakers that privacy is a bipartisan issue, that everyones on board, that no one likes the idea of Yeah, they dont do anything. And I chart it in the book, but strange political bedfellows coming together again and again to talk about facial recognition technology and its harms to civil liberties. Most recently, a hearing led by John Lewis who has since passed but civil rights leader, he was leading the impeachment investigation into Trump and he partnered with Jim Jordan and Mark Meadows, huge Trump supporters in Congress. And they had this hearing about facial recognition technology, and they said it. They said, Theres not much we agree on here, but this is a topic that unites us. We all believe we need to protect citizens from invasions of their privacy. And then nothing happens.Its just so gridlocked at the national level that I dont have a lot of hope for something coming from there. But we have seen a lot of activity on this at the local level and at the state level from BIPA and maybe other states would pass something like that to just state privacy laws that give you the right to access information that a company holds on you and delete it. So if you live in California or Connecticut or Virginia or Colorado, you can go to Clearview and say, Hey, I want to see my results. And if you dont like being in their database, you can say, Delete me from your database.Do you think enough people know that they can do that? If I lived in one of those states, I would be doing that every week and just being like, Who knows about me? Delete it. There should be a secondary economy of companies just offering that service to people. There already are, in some cases. There is DeleteMe that just deletes you from various things. Is that the solution here, that theres just a market for privacy, and you can be on one side of it or the other?California, actually as part of its law, has this requirement that a company has to disclose how many times people use this right against them. And so I was looking at Clearviews privacy page to find out. California has millions and millions and millions of people, and Clearview, last year I think, got something like 451 requests for deletion there, which seems quite tiny. I would think it would be higher than that.Yeah. Thats just tech reporters. Thats just people seeing if they can do it.Yeah, mostly its probably tech reporters and privacy academics and students who are doing it as their homework for some class.Legislative aids making sure the law is in compliance.Is that just people dont know, and there needs to be a bunch of education? Is that, eventually people will realize, This is happening, and I should go and proactively try to stop it? What keeps people from wanting to protect their privacy?I just think people dont anticipate the harms. I think thats whats so hard about privacy is that you dont realize what is going to hurt you, what information is out there is going to harm you until it happens. Until you do get wrongfully arrested for a crime because a police officer made a mistake and identified you with Clearview. Its hard to see it coming. You dont realize until after its happened.Theres the flip side of this. Its where we started. The big companies have had the opportunity to do it for a long time. This is a very processor-intensive task. Theyre running these high-end machine learning algorithms. You need all this stuff. Amazon could do it, Google can do it, Facebook can do it. Apple could do it if they wanted to. But they dont. They have stopped themselves, and they havent even stopped themselves in the way they usually stop themselves. Theyre not saying, Hey, you should pass a law, or were definitely going to do this, which is what theyre effectively doing with AI right now. Theyre just not doing it. I cant recall another time when all of those companies have just not done something, and theyve allowed one startup to go take all the heat. Is there a reason for that? Is there just an ineffable morality inside of all these companies thats keeping them from doing it? Or is there a reason?I think facial recognition technology is more controversial. Theres just something that is specifically toxic about it. I do think theres worry. I think theres worry about legality. Illinois has this law around use of face prints. So does Texas.Is it really just Illinois is keeping everyone from doing it?I remember a few years ago when Google had that Art Selfie app. Do you remember that? You could take your photo, and it would tell you what masterpiece you look like. And it didnt work in Illinois, and it didnt work in Texas. They geofenced them off because it is a really expensive law to break. So I think thats part of it.They have introduced this technology in ways. Like, when I go on my iPhone, I can search all my photos by face and see them all. Thats a convenient tool, and I think their users like it. Maybe its just we, as a society, arent asking for the ability to just recognize everybody at a cocktail party. Andrew Bosworth at Meta has talked a few years ago about how he would love to give us facial recognition capabilities in glasses, and it would be great at a cocktail party to put a name to a face, or blind users or face blind people could use it. But that hes worried maybe society doesnt want this. Maybe its illegal.No, so I think this is the killer app for these glasses. I would wear the headset all day. You could put me in one of their silly VR headsets all day long if I could do faces and names. Im horrible at faces and names. I would probably be historys greatest politician if I could just remember peoples names. I believe this about myself because its how I excuse the fact that Im really bad at faces and names. Thats the killer app. You wear the glasses, theyre expensive, whatever, but it can just tell you who other people are. I know that people would buy that product without a seconds hesitation. The societal cost of that product seems like its too high. I dont know how to build that product in a privacy-sensitive way. And no one Ive ever interviewed on this show has ever offered me a solution.But the market wants that product, right? The version of this that I imagine could be possible would be like in the way that we set the privacy of our Facebook profiles or Instagram pages, we say, This is public, or, This is visible only to friends, or, Friends of friends can see the content. I could imagine a version of Metas augmented reality glasses where you could set the privacy of your face and say, Okay, Im willing to opt in to facial recognition technology, and I want my face to be public. I want anybody whos wearing these glasses to know who I am. Or, You know my social graph. I want to be recognizable by people Im connected to on Facebook or Instagram or Threads. Or, I want to be recognizable to friends of friends.I could imagine that world in which we have the ability to say how recognizable we want our friends to be because the technology is offered by a company that knows our social graph. I just wonder, if that happens, how many people opt in to that? And then, do you get completely stigmatized if youre a person who says, I want to be private all the time?It feels like eating too much sugar or something. Theres something happening here where, of course, I want everybody at the party to know who I am and what my interests are so they can come talk to me. But 10 years down the line, Im sitting in a jail for a week waiting for my lawyer to tell the cops, That wasnt me. Those are so disconnected in time and harm that Im just not sure how to communicate that to people.Right. Or you set your face to public because youre like, This is great for advertising my business. But then youre out at a bar with your sidepiece and you forget that your face is public, and now you are in trouble. [Laughs] Its just hard to anticipate the harms. Sometimes the benefits are more obvious and sometimes the harms are more obvious. Maybe with facial recognition technology, these companies havent released it because they do see the harms more clearly than the benefits.That is one of the first times anyone has ever claimed that tech companies see the harms more clearly than the benefits.Yeah, Im not certain about that.That I can recall on the show, actually. Even the executives from the tech companies.So lets talk about where this goes. Weve established that Clearview is a pretty singular company. Theyve built a technology that other people could have built, but for various reasons most notably the governments of Europe and Illinois, two governments that you often think of together other people arent in this market. But the cops really like this technology. Dads looking at their daughters on dates in restaurants appear to really like this technology. Theres a market for it; theres a demand for it. The harms are pretty hard to explain to people. Is this going to keep happening? Are there going to be more state-level laws or European Union laws? Is everyone just waiting to see what happens with Clearview? What does Clearview think is going to happen?I think Clearview wants to keep selling this to law enforcement, and they are. I think that the question we need to ask ourselves right now is: how widely deployed do we want this to be? And its a question at the government level. Do we want police only using this to solve crimes that have already happened? Or do we want to roll out facial recognition technology on cameras around the country so that you can get real-time alerts when there is a fugitive on the loose? I was thinking about this when that guy escaped in Pennsylvania, and it just felt like we were looking for him for forever. And I can imagine a case like that being, they say, If we just put facial recognition on all the cameras, then we could find them in an instant. So yeah, that question of do we deploy it more widely? Do we all have an app like this on our phone? Or do we set more rules, where we control whether were in these databases, we control when this is used for our benefit versus on us?And there are so many questions there because, if we do roll it out more widely, its just going to be used against some people more than others. Were already seeing it in the police use. We know of a handful of wrongful arrests where people have been arrested, put in jail for the crime of looking like someone else. And in every case, its involved a person who is Black. So already, were seeing when it goes wrong. Its going wrong for people who are Black. Facial recognition technology is being used more on them. We need to make some decisions right now of what we want the world to look like and whether we want our faces tracked all the

time. I hope the answer is no. I hope that doesnt happen because I do think we need zones of privacy. I dont want to live in a panopticon.Were already seeing a bunch of private uses of this, maybe not the panopticon version, but the Hey, the sports stadium has facial recognition technology to track the person on their way out the door. Madison Square Garden famously is tracking lawyers from law firms that are suing the Dolan family. Thats happening. Is that going to keep happening? Do some of these laws affect that, too? Or are we going to have little zones of privacy and little zones of not privacy?Yeah, so Madison Square Garden installed facial recognition, as many shops now have done. Like grocery stores use this to keep out shoplifters, and Madison Square Garden was saying, We want to keep out stalkers during concerts. We want to keep out people whove been violent in the stadium before. And then, in the last year, they started using it to ban lawyers who worked at firms that had sued Madison Square Garden because the owner, James Dolan, didnt like them and how much money they cost him. But Madison Square Garden has done this for all their properties in New York Beacon Theatre, Radio City Music Hall but they have a theater in Chicago, and they cant do that there because Illinois has this law. You cant use lawyers face prints without their permission.So again, laws work, and we could pass more of them if we want to. But yeah, companies are definitely rolling out facial recognition technology on us to deter crime. And then, as a service. And I do see this in a lot of arenas now: to go through the concession line faster, just pay with your face for your Coke. And thats part of the normalization of the technology, and I think thats fine. If youre comfortable with that, and it makes your life easier, thats great. But I think we should have limits on it so that they cant just start building some crazy face database and using it for something else. I really think we need to put limits on the technology to protect us.Well if Ive learned anything, its that I need to move back home to Chicago.Thats my takeaway from this episode of Decoder. I left there a long time ago, but maybe its time to go back. Kash, I am such a huge fan of your work. I love the book. I think its out now. People should go read it. Tell them where they can buy it.They can buy it anywhere. Amazon, if youre into the tech giants. You can get it at Barnes & Noble, at Bookshop.I just like making people say they can buy it at Amazon. Thats just a troll I do at the end of every episode. This has been great. I really recommend the book.I like Bookshop.org because it supports your independent bookstore, which is great.Thank you so much for being on Decoder, Kash. This was great.Thank you so much. It was great to be here.A podcast about big ideas and other problems.SUBSCRIBE NOW!Follow topics and authors from this story to see more like this in your personalized homepage feed and to receive email updates.Nilay PatelPosts from this author will be added to your daily email digest and your homepage feed.See All by Nilay PatelPosts from this topic will be added to your daily email digest and your homepage feed.See All AIPosts from this topic will be added to your daily email digest and your homepage feed.See All DecoderPosts from this topic will be added to your daily email digest and your homepage feed.See All PodcastsPosts from this topic will be added to your daily email digest and your homepage feed.See All PolicyPosts from this topic will be added to your daily email digest and your homepage feed.See All PrivacyPosts from this topic will be added to your daily email digest and your homepage feed.See All Tech

American facial recognition software companyClearview AI, Inc.Company typePrivateIndustryFacial recognition, softwareFounded2017; 8years ago(2017)[1]FoundersHoan Ton-ThatRichard SchwartzHeadquartersManhattan, New York City, United StatesAreas servedGlobally excluding EU, UK, NZ, Canada, AustraliaKey peopleHal Lambert, Richard SchwartzProductsClearview AI Software Clearview AI Search EngineWebsiteclearview.aiClearview AI, Inc. is an American facial recognition company, providing software primarily to law enforcement and other government agencies.[2] The company's algorithm matches faces to a database of more than 20 billion images collected from the Internet, including social media applications.[1] Founded by Hoan Ton-That, Charles C. Johnson,[3] and Richard Schwartz, the company maintained a low profile until late 2019, until its usage by law enforcement was first reported.[4]Use of the facial recognition tool has been controversial. Several U.S. senators have expressed concern about privacy rights and the American Civil Liberties Union (ACLU) has sued the company for violating privacy laws on several occasions. U.S. police have used the software to apprehend suspected criminals.[5][6][7] Clearview's practices have led to fines and bans by EU nations for violating privacy laws, and investigations in the U.S. and other countries.[8][9][10] In 2022, Clearview reached a settlement with the ACLU, in which they agreed to restrict U.S. market sales of facial recognition services to government entities.In 2020, a data breach of Clearview AI demonstrated 2,200 organizations in 27 countries had accounts with facial recognition searches.[11]Clearview AI was founded in 2017 by Hoan Ton-That and Richard Schwartz after transferring the assets of another company, SmartCheckr, which the pair originally founded in 2017 alongside Charles C. Johnson.[12][4] The company was founded in Manhattan after the founders met at the Manhattan Institute.[1] The company initially raised $8.4 million from investors including Kirenaga Partners and Peter Thiel.[13] Additional fundraising, in 2020, collected $8.625 million in exchange for equity. The company did not disclose investors in the second round. In 2021, another fundraising round received $30 million.[14] Early use of Clearview's app was given to potential investors in their Series A fundraising round. Billionaire John Catsimatidis used it to identify someone his daughter dated and piloted it at one of his Gristedes grocery markets in New York City to identify shoplifters.[15][16]In October 2020, a company spokesperson claimed that Clearview AI's valuation was more than $100 million.[17] The company announced its first chief strategy officer, chief revenue officer, and chief marketing officer in May 2021. Devesh Ashra, a former deputy assistant secretary with the United States Department of the Treasury, became its chief strategy officer. Chris Metaxas, a former executive at LexisNexis Risk Solutions, became its chief revenue officer. Susan Crandall, a former marketing executive at LexisNexis Risk Solutions and Motorola Solutions, became its chief marketing officer.[18] Devesh Ashra and Chris Metaxas left the company in 2021.[14] In August 2021, Clearview AI announced the formation of an advisory board including Raymond Kelly, Richard A. Clarke, Rudy Washington, Floyd Abrams, Lee S. Wolosky, and Owen West.[19] The company claimed to have scraped more than 10 billion images as of October 2021.[20] In May 2022, Clearview AI announced that it would be expanding sales of its facial recognition software to schools and lending platforms outside the U.S.[21]Clearview AI hired a notable legal team to defend the company against several lawsuits that threatened their business model. Their legal staff includes Tor Ekeland, Lee S. Wolosky, Paul Clement, Floyd Abrams, and Jack Mulcaire.[22][1][23] Abrams stated the issue of privacy rights versus free speech in the First Amendment could reach the Supreme Court.[22]On February 19, 2025, following the resignation of Ton-That in December 2024, Clearview AI appointed Hal Lambert and Richard Swartz as CEOs. Lambert and Swartz were early investors in the company. Lambert previously did fundraising for the Trump presidential campaigns. In a separate statement Ton-That said he would remain a board member.[24]Clearview AI provides facial recognition software where users can upload an image of a face and match it against their database.[25] The software then supplies links to where the "match" can be found online.[26] The company operated in near secrecy until the release of an investigative report in The New York Times titled "The Secretive Company That Might End Privacy as We Know It" in January 2020. It maintained this secrecy by publishing fake information about the company's location and employees and erasing social media for the founders.[4][1][27] Citing the article, over 40 tech and civil rights organizations sent a letter to the Privacy and Civil Liberties Oversight Board (PCLOB) and four congressional committees, outlining their concerns with facial recognition and Clearview, and asking the PCLOB to suspend use of facial recognition.[28][29][30][1]Clearview served to accelerate a global debate on the regulation of facial recognition technology by governments and law enforcement.[31][32] Law enforcement officers have stated that Clearview's facial recognition is far superior in identifying perpetrators from any angle than previously used technology.[33] After discovering Clearview AI was scraping images from their site, Twitter sent a cease-and-desist letter to Clearview, insisting that they remove all images as scraping is against Twitter's policies.[34] On February 5 and 6, 2020, Google, YouTube, Facebook, and Venmo sent cease and desist letters as it is against their policies.[35][36] Ton-That responded in an interview that there is a First Amendment right to access public data. He later stated that Clearview has scraped over 50 billion images from across the web.[31][37][38]The New Zealand Police used it in a trial after being approached by Clearview's Marko Jukic in January 2020. Jukic said it would have helped identify the Christchurch mosque shooter had the technology been available. The usage of Clearview's software in this case raised strong objections once exposed, as neither the users' supervisors or the Privacy Commissioner were aware or approved of its use. After it was revealed by RNZ, Justice Minister Andrew Little stated, "It clearly wasn't endorsed, from the senior police hierarchy, and it clearly didn't get the endorsement from the [Police] Minister... that is a matter of concern."[39][40]Clearview's technology was used for identifying an individual at a May 30, 2020 George Floyd police violence protest in Miami, Florida. Miami's WTVJ confirmed this, as the arrest report only said she was "identified through investigative means". The defendant's attorney did not even know it was with Clearview. Ton-That confirmed its use, noting that it was not being used for surveillance, but only to investigate a crime.[41]In December 2020, the ACLU of Washington sent a letter to Seattle mayor Jenny Durkan, asking her to ban the Seattle Police Department from using Clearview AI.[42] The letter cited public records retrieved by a local blogger, which showed one officer signing up for and repeatedly logging into the service, as well as corresponding with a company representative. While the ACLU letter raised concerns that the officer's usage violated the Seattle Surveillance Ordinance, an auditor at the City of Seattle Office of the Inspector General argued that the ordinance was designed to address the usage of surveillance technologies by the Department itself, not by an officer without the Department's knowledge.[43]After the January 6 riot at the United States Capitol, the Oxford Police Department in Alabama used Clearview's software to run a number of images posted by the Federal Bureau of Investigation in its public request for suspect information to generate leads for people present during the riot. Photo matches and information were sent to the FBI who declined to comment on its techniques.[6]In March 2022, Ukraine's Ministry of Defence began using Clearview AI's facial recognition technology "to uncover Russian assailants, combat misinformation and identify the dead". Ton-That also claimed that Ukraine's MoD has "more than 2 billion images from the Russian social media service VKontakte at its disposal".[44] Ukrainian government agencies used Clearview over 5,000 times as of April 2022.[45][46] The company provided these accounts and searches for free.[47]In a Florida case, Clearview's technology was used by defense attorneys to successfully locate a witness, resulting in the dismissal of vehicular homicide charges against the defendant.[48]Law enforcement use of the facial recognition software grew rapidly in the United States. In 2022 more than one million searches were conducted. In 2023, this usage doubled.[38]Clearview AI encouraged user adoption by offering free trials to law enforcement officers rather than departments as a whole. The company additionally used its significant connections to the Republican Party to connect with police departments.[1][49] In onboarding emails, new users were encouraged to go beyond running one or two searches to "[s]ee if you can reach 100 searches".[50] During 2020, Clearview sold their facial recognition software for one tenth the cost of competitors.[4]Clearview's marketing claimed their facial recognition led to a terrorist arrest. The identification was submitted to the New York Police Department tip line.[51] Clearview claims to have solved two other New York cases and 40 cold cases, later stating they submitted them to tip lines. NYPD stated they have no institutional relationship with Clearview, but their policies do not ban its use by individual officers. In 2020, thirty NYPD officers were confirmed to have Clearview accounts.[4] In April 2021, documents obtained by the Legal Aid Society under New York's Freedom Of Information Law demonstrated that Clearview had collaborated with the NYPD for years, contrary to past NYPD denials.[52] Clearview met with senior NYPD leadership and entered into a vendor contract with the NYPD.[50] Clearview came under renewed scrutiny for enabling officers to conduct large numbers of searches without formal oversight or approval.[52][50]The company was sent a cease and desist letter from the office of New Jersey Attorney General Gurbir Grewal after including a promotional video on its website with images of Grewal.[53] Clearview had claimed that its app played a role in a New Jersey police sting. Grewal confirmed the software was used to identify a child predator, but he also banned the use of Clearview in New Jersey. Tor Ekeland, a lawyer for Clearview, confirmed the marketing video was taken down the same day.[5][54]In March 2020, Clearview pitched their technology to states for use in contact tracing to assist with the COVID-19 pandemic.[55][56] A reporter found Clearview's search could identify him while he covered his nose and mouth like a COVID mask would.[47] The idea brought criticism from US senators and other commentators because it seemed the crisis was being used to push unreliable tools that violate personal privacy.[57][58]Contrary to Clearview's initial claims that its service was sold only to law enforcement, a data breach in early 2020 revealed that numerous commercial organizations were on Clearview's customer list. For example, Clearview marketed to private security firms and to casinos.[59] Additionally, Clearview planned expansion to many countries, including authoritarian regimes.[60] Senator Edward J. Markey wrote to Clearview and Ton-That, stating "Widespread use of your technology could facilitate dangerous behavior and could effectively destroy individuals' ability to go about their daily lives anonymously." Markey asked Clearview to detail aspects of its business, in order to understand these privacy, bias, and security concerns.[34][61] Clearview responded through an attorney, declining to reveal information.[62] In response to this, Markey wrote a second letter, saying their response was unacceptable and contained dubious claims, and that he was concerned about Clearview "selling its technology to authoritarian regimes" and possible violations of COPPA.[9][63] Senator Markey wrote a third letter to the company with concerns, stating "this health crisis cannot justify using unreliable surveillance tools that could undermine our privacy rights." Markey asked a series of questions about what government entities Clearview has been talking with, in addition to unanswered privacy concerns.[57]Senator Ron Wyden voiced concerns about Clearview and had meetings with Ton-That cancelled on three occasions.[64][9] In April 2021, Time magazine listed Clearview AI as one of the 100 most influential companies of the year.[65]In October 2021 Clearview submitted its algorithm to one of two facial recognition accuracy tests conducted by the National Institute of Standards and Technology (NIST) every few months. Clearview ranked amongst the top 10 of 300 facial recognition algorithms in a test to determine accuracy in matching two different photos of the same person. Clearview did not submit to the NIST test for matching an unknown face to a 10 billion image database, which more-closely matches the algorithm's intended purpose. This was the first third-party test of the software.[20]Clearview, at various times throughout 2020, has claimed 98.6%, 99.6%, or 100% accuracy. However, these results are from tests conducted by people affiliated with the company and have not used representative samples of the population.[31][66][67]In 2021, Clearview announced that it was developing "deblur" and "mask removal" tools to sharpen blurred images and envision the covered part of an individual's face. These tools would be implemented using machine learning models that fill in the missing details based on statistical patterns found in other images. Clearview acknowledged that deblurring an image and/or removing a mask could potentially make errors more frequent and would only be used to generate leads for police investigations.[37]Assistant Chief of Police of Miami, Armando Aguilar, said in 2023 that Clearview's AI tool had contributed to the resolution of several murder cases, and that his team had used the technology around 450 times a year. Aguilar emphasized that they do not make arrests based on Clearview's matches alone, and instead use the data as a lead and then proceed via conventional methods of case investigation.[26]Several cases of mistaken identity using Clearview facial recognition have been documented, but "the lack of data and transparency around police use means the true figure is likely far higher." Ton-That claims the technology has approximately 100% accuracy, and attributes mistakes to potential poor policing practices. Ton-That's claimed accuracy level is based on mugshots and would be affected by the quality of the image uploaded.[26]Clearview AI experienced a data breach in February 2020 which exposed its list of customers. Clearview's attorney, Tor Ekeland stated the security flaw was corrected.[68] In response to the leaks, the United States House Committee on Science, Space, and Technology sent a letter to the company requesting further insight into their bio-metric and security practices.[69]While Clearview's app is only supposed to be privately accessible to customers, the Android application package and iOS applications were found in unsecured Amazon S3 buckets.[70] The instructions showed how to load an enterprise (developer) certificate so the app could be installed without being published on the App Store. Clearview's access was suspended, as it was against Apple's terms of service for developers, and as a result the app was disabled.[71] In addition to application tracking (Google Analytics, Crashlytics), examination of the source code for the Android version found references to Google Play Services, requests for precise phone location data, voice search, sharing a free demo account to other users, augmented reality integration with Vuzix, and sending gallery photos or taking photos from the app itself. There were also references to scanning barcodes on a drivers license and to RealWear.[72]In April 2020, Mossab Hussein of SpiderSilk, a security firm, discovered Clearview's source code repositories were exposed due to misconfigured user security settings. This included secret keys and credentials, including cloud storage and Slack tokens. The compiled apps and pre-release apps were accessible, allowing Hussein to run the macOS and iOS apps against Clearview's services. Hussein reported the breach to Clearview but refused to sign a non-disclosure agreement necessary for Clearview's bug bounty program. Ton-That reacted by calling Hussein's disclosure of the bug as an act of extortion. Hussein also found 70,000 videos in one storage bucket from a Rudin Management apartment building's entrance.[73]Clearview also operates a secondary business, Insight Camera, which provides AI-enabled security cameras. It is targeted at "retail, banking and residential buildings". Two customers have used the technology, United Federation of Teachers and Rudin Management.[74][75] The website for Insight Camera was taken down following BuzzFeed's investigation into the connection between Clearview AI and Insight Camera.[76]Following a data leak of Clearview's customer list, BuzzFeed confirmed that 2,200 organizations in 27 countries had accounts with activity. BuzzFeed has the exclusive right to publish this list and has chosen not publish it in its entirety.[11] Clearview AI claims that at least 600 of these users are police departments. These are primarily in the U.S. and Canada, but Clearview has expanded to other countries as well.[4] Although the company claims their services are for law enforcement, they have had contracts with Bank of America, Kohls, and Macy's. Several universities and high schools have done trials with Clearview.[11] The list below highlights particularly notable users.American law enforcement and governmentIllinois Secretary of State (almost 9,000 searches, has been using since approx Nov 2019)[77]New York Police Department (over 11,000 searches by over 30 accounts, most of any user)[11]Raleigh Police Department, North Carolina (a paid client, then its use was banned, then continued to use trial access after the ban)[11]Atlanta Police Department, ($6000 one year contract)[4]Chicago Police Department (a paid customer, over 1,500 searches on 30 accounts, paid $49,875 for a two-year license)[11]New York State Police (a paid customer, $15,000 for licenses)[11]Indiana State Police (a paid customer, over 5,700 searches)[11]Miami Police Department (over 3,000 searches)[11]Texas Department of Public Safety (signed a $24k contract in December 2019)[57]FBI (5,700 searches)[11]BATF (2,100 searches)[11]US Secret Service (5,600 searches)[11]DEA (2,000 searches)[11]Department of Homeland Security[11]U.S. Air Force (signed a $50k contract in December 2019)[57]U.S. Customs and Border Protection (not a paid customer, 280 accounts, 7,500 searches)[11]U.S. Immigration and Customs Enforcement[11]Virginia Beach Police[78]International law enforcementVadodara City Police, part of the Gujarat Police in Vadodara, India[79][11]Australian Federal PoliceAustralian Centre to Counter Child Exploitation (7 trial accounts, Nov 2019 Jan 2020)[80]Metropolitan Police Service, London, UK[81]30 law enforcement agencies in Canada[11]Royal Canadian Mounted Police (paying customer, used for four months in the National Child Exploitation Crime Centre and by others as a trial)[82][11]Ontario Provincial Police[83][84]Edmonton Police Service, Edmonton, Alberta (used by three officers without department approval)[85]London Police Service, London, Ontario (trial by seven officers)[86][87]Toronto Police Service (tested from October 2019 to February 2020)[82][88][89][11]Sweden law enforcement[90]Ministry of Defence of Ukraine[44]New Zealand Police (trialed Jan 2020)[39]Clearview AI has had its business model challenged by several lawsuits in multiple jurisdictions. It responded by defending itself, settling in some cases, and exiting several markets. The company's claim of a First Amendment right to public information has been disputed by privacy lawyers such as Scott Skinner-Thompson and Margot Kaminski, highlighting the problems and precedents surrounding persistent surveillance and anonymity.[36][91] Former New York City Police Commissioner and executive chairman of Teneo Risk Chief Bill Bratton challenged privacy concerns and recommended strict procedures for law enforcement usage in an op-ed in New York Daily News.[92]After the release of The New York Times January 2020 article, lawsuits were filed by the states of Illinois, California, Virginia and New York, citing violations of privacy and safety laws.[93] Most of the lawsuits were transferred to New York's Southern District.[94] Two lawsuits were filed in state courts; in Vermont by the attorney general and in Illinois on behalf of the American Civil Liberties Union (ACLU), which cited a statute that forbids the corporate use of residents' faceprints without explicit consent. Clearview countered that an Illinois law does not apply to a company based in New York.[22]In response to a class action lawsuit filed in Illinois for violating the Biometric Information Privacy Act (BIPA), in May 2020 Clearview stated that they instituted a policy to stop working with non-government entities and to remove any photos geolocated in Illinois.[95][96][77] On May 28, 2020, ACLU and Edelson filed a new suit Clearview in Illinois using the BIPA.[97][98] Clearview agreed to a settlement in June 2024, offering 23% of the company (valued at $52 million at the time) rather than a cash settlement, which was likely to bankrupt the company.[99]In May 2022, Clearview agreed to settle the 2020 lawsuit from the ACLU. The settlement prohibited the sale of its facial recognition database to private individuals and businesses.[100]In the Vermont case, Clearview AI invoked Section 230 immunity. The court denied the use of Section 230 immunity in this case because Vermont's claims were "based on the means by which Clearview acquired the photographs" rather than third party content.[101]In July 2020, Clearview AI announced that it was exiting the Canadian market amidst joint investigations into the company and the use of its product by police forces.[102] Daniel Therrien, the Privacy Commissioner of Canada condemned Clearview AI's use of scraped biometric data: "What Clearview does is mass surveillance and it is illegal. It is completely unacceptable for millions of people who will never be implicated in any crime to find themselves continually in a police lineup."[103] In June 2021, Therrien found that the Royal Canadian Mounted Police had broken Canadian privacy law through hundreds of illegal searches using Clearview AI.[104]In January 2021, Clearview AI's biometric photo database was deemed illegal in the European Union (EU) by the Hamburg Data Protection Authority (DPA).[105] The Hamburg DPA ordered deletion of biometric data for a specific affected person. The authority stated that the General Data Protection Regulation (GDPR) was applicable despite the fact that Clearview AI has no European branch offices.[106] The data protection advocacy organization, European Center for Digital Rights (NOYB), criticized the Hamburg DPA's decision, as the DPA order protected only one individual complainant instead of banning the collection of any European resident's photos.[105] In March 2020, Hamburg DPA requested Clearview AI's customer list, as data protection obligations would apply to customers.[107]In May 2021, the company was subject to legal complaints filed in Austria, France, Greece, Italy, and the United Kingdom for violating European privacy laws in its method of documenting and collecting Internet data.[108] In November 2021, Clearview received a provisional notice by the UK's Information Commissioner's Office (ICO) to stop processing UK citizens' data, citing a range of alleged breaches. Clearview claimed that the ICO's allegations were factually inaccurate as the company "does not do business in the UK, and does not have any UK customers at this time". The BBC reported in May 2023 that Clearview had been fined "more than 7.5m by the UK's privacy watchdog and told to delete the data of UK residents" including all facial recognition data of UK residents.[109] This fine marked the fourth of its kind imposed upon Clearview, after similar orders and fines were issued by authorities in Australia, France, and Italy.[10] However, in October 2023, the UK fine was overturned following a Clearview appeal based on the jurisdiction of the ICO over acts of foreign governments.[110]In September 2024, Clearview AI was fined 30.5 million by the Dutch Data Protection Authority (DDPA) for constructing what the agency described as an illegal database.[111] The DDPA ruled that Clearview AI unlawfully collected facial images, including those of Dutch citizens, without obtaining their consent. This practice constitutes a significant violation of the EU's GDPR due to the intrusive nature of facial recognition technology and the lack of transparency regarding the use of individuals' biometric data.[112]Companies portalhiQ Labs v. LinkedInDataWorks Plus

^ a b c d e f g Hill, Kashmir (January 18, 2020). "The Secretive Company That Might End Privacy as We Know It". The New York Times. ISSN0362-4331. Retrieved January 18, 2020.^ What We Learned About Clearview AI and Its Secret 'Co-Founder'^ Luke O'Brien. (May-June 2025) "Clear and present danger". Mother Jones magazine website Vol. 50, no. 3. P.21. Retrieved 14 April 2025.^ a b c d e f g "Clearview AI Says Its Facial Recognition Software Identified A Terrorism Suspect. The Cops Say That's Not True". BuzzFeed News. January 23, 2020. Retrieved January 23, 2020.^ a b "New Jersey cops told to halt all use of controversial facial-recognition technology". nj. January 24, 2020. Retrieved January 26, 2020. Tor Ekeland, a Clearview lawyer, wrote in an email that they would take the video down, and it was no longer at the top of the company's website Friday evening.^ a b Hill, Kashmir (January 9, 2021). "The facial-recognition app Clearview sees a spike in use after Capitol attack". The New York Times.^ Council, Jared (January 8, 2021). "Local Police Force Uses Facial Recognition to Identify Capitol Riot Suspects". The Wall Street Journal.^ "Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani". gpdp.it (in Italian). Retrieved February 10, 2024.^ a b c "Senators Are Probing Clearview AI On The Use Of Facial Recognition By Gulf States And International Markets". BuzzFeed News. March 4, 2020. Retrieved March 5, 2020.^ a b "Clearview AI ordered to delete facial recognition data belonging to UK residents". The Verge. May 26, 2022. Retrieved May 26, 2022.^ a b c d e f g h i j k l m n o p q r s t McDonald, Ryan Mac, Caroline Haskins, Logan (February 28, 2020). "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA". BuzzFeed News. Retrieved June 13, 2024.{{cite web}}: CS1 maint: multiple names: authors list (link)^ Johnson v Clearview, 23 Civ 2441 (UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK May 20 2024).^ Mac, Ryan; Sacks, Brianna (September 24, 2020). "Controversial Facial Recognition Firm Clearview AI Raised $8.6 Million". BuzzFeed News. Retrieved September 24, 2020.^ a b Dastin, Jeffery; Dave, Paresh. "EXCLUSIVE Facial recognition startup Clearview AI drops sales chief, chunk of staff -sources". Reuters. Reuters. Retrieved June 14, 2024.^ "NYT: Billionaire with ties to St. Petersburg tested facial recognition app". Tampa Bay Times. Retrieved March 8, 2020.^ Hill, Kashmir (March 5, 2020). "Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich". The New York Times. Retrieved March 8, 2020.^ Somerville, Heather (October 20, 2020). "Facial-Recognition Startup Clearview Moves to Limit Risk of Police Abuse". The Wall Street Journal. Retrieved November 3, 2020.^ "Three New Faces Join Clearview AI". Yahoo! Finance. May 18, 2021.^ "Clearview AI Announces Formation of Advisory Board" (Press release). New York: Business Wire. The LAKPR Group Inc. August 18, 2021. Retrieved August 26, 2021.^ a b Hill, Kashmir (October 28, 2021). "Clearview AI finally takes part in a federal accuracy test". The New York Times. Retrieved December 1, 2021.^ Paresh Dave (May 24, 2022). "Clearview AI's facial recognition tool coming to apps, schools". Reuters. Retrieved June 19, 2022.^ a b c "Facial Recognition Start-Up Mounts a First Amendment Defense in Privacy Suits". The New York Times. August 11, 2020. Retrieved August 11, 2020.^ Vallance, Chris (October 18, 2023). "Face search company Clearview AI overturns UK privacy fine". BBC. BBC. Retrieved June 15, 2024.^ Jeans, David. "Clearview AI's CEO Resigns As Facial Recognition Company Focuses On Trump 'Opportunities'". Forbes. Archived from the original on February 20, 2025. Retrieved February 20, 2025.^ Richman, Josh (March 26, 2024). "Podcast Episode: About Face (Recognition)". Electronic Frontier Foundation. Retrieved August 8, 2024.^ a b c Clayton, James; Derico, Ben (March 27, 2023). "Clearview AI used nearly 1m times by US police, it tells the BBC". BBC News. Archived from the original on September 23, 2023. Retrieved October 6, 2023.^ Ryssdal, Kai (September 19, 2023). "The facial recognition software cops are raving about". Marketplace. Event occurs at 07:00. APM. Marketplace.org. Retrieved September 19, 2023. I see you have a lot of photos on the internet you should be in the app but you're not here... A couple of minutes later he said he got a call from someone who worked for Clearview AI and they wanted to know why he'd been running my photo.^ "EPIC PCLOB letter" (PDF). Electronic Privacy Information Center. Retrieved January 27, 2020.^ "U.S. Board Should Seek Facial Recognition Halt, Groups Say (1)". Bloomberg Law. Retrieved January 27, 2020. 'Obvious problems with bias and discrimination in the systems' show the need for a moratorium, 40 organizations wrote in a letter to the Privacy and Civil Liberties Oversight Board.^ Thomas, By Owen (January 22, 2020). "The person behind a privacy nightmare has a familiar face". San Francisco Chronicle. Retrieved January 23, 2020. I wrote about Ton-That in February 2009 ('scathingly,' Hill writes), when he was living in San Francisco, developing first Facebook and then iPhone apps. He made the news for creating ViddyHo, a website that tricked users into sharing access to their Gmail accounts a hacking technique known as 'phishing' and then spammed their contacts on the Google Talk chat app. (The episode does not appear on Ton-That's sanitized personal website.)^ a b c Errol Barnett (February 5, 2020). "Google, YouTube and Venmo send cease-and-desist letters to facial recognition app that helps law enforcement". CBS News. Retrieved February 6, 2020.^ Ryan Mellino (November 28, 2023). Regulators Should Use Existing Legal Tools to Rein in Clearview AI's Abuses of Our Personal Privacy Rights (PDF) (Report). Consumer Watchdog. pp.23. Retrieved June 7, 2024.^ Linder, Courtney (January 22, 2020). "This App Is a Dangerous Invasion of Your Privacyand the FBI Uses It". Popular Mechanics. Retrieved February 11, 2020.^ a b Hill, Kashmir (January 23, 2020). "Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos". The New York Times. Retrieved January 26, 2020. Twitter sent a letter this week to the small start-up company, Clearview AI, demanding that it stop taking photos and any other data from the social media website "for any reason" and delete any data that it previously collected, a Twitter spokeswoman said. The cease-and-desist letter...accused Clearview of violating Twitter's policies.^ Igor Bonifacic (February 5, 2020). "Google tells facial recognition startup Clearview AI to stop scraping photos". Engadget. Retrieved February 6, 2020. Following Twitter, Google and YouTube have become the latest companies to send a cease-and-desist letter to Clearview AI, the startup behind a controversial facial recognition program that more than 600 police departments across North American use.^ a b Ng, Alfred. "Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection". CNET. Retrieved February 11, 2020.^ a b Will Knight. "Clearview AI Has New Tools to Identify You in Photos". Wired.^ a b Smalley, Suzanne. "Law enforcement searches of Clearview AI facial recognition doubled in past year". therecord.media. Recorded Future News. Retrieved July 19, 2024.^ a b "Police trial of facial recognition technology 'a matter of concern' Andrew Little". RNZ. May 13, 2020. Retrieved May 13, 2020.^ "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI". RNZ. May 15, 2020. Retrieved May 15, 2020. Official emails released to RNZ show how police first used the technology: by submitting images of wanted people who police say looked "to be of Mori or Polynesian ethnicity", as well as "Irish roof contractors".^ Connie Fossi; Phil Prazan (August 17, 2020). "Miami Police Used Facial Recognition Technology in Protester's Arrest". NBC 6 South Florida. Retrieved August 18, 2020. The NBC 6 Investigators found police used the facial recognition program Clearview AI to find her.^ Graham, Nathalie. "ACLU Asks Durkan to Ban Use of Facial Recognition Software at SPD". The Stranger. Retrieved April 14, 2021.^ Kiefer, Paul (December 3, 2020). "ACLU Calls on Durkan to Ban Facial Recognition Software After Possible SPD Violation". PubliCola. Retrieved April 14, 2021.^ a b Dave, Paresh; Dastin, Jeffrey (March 13, 2022). "Exclusive: Ukraine has started using Clearview AI's facial recognition during war". Reuters. Retrieved March 14, 2022.^ Kashmir Hill (April 7, 2022). "Facial Recognition Goes to War". NY Times. Retrieved April 14, 2022.^ Al-Nabulsi, Jamal; Turab, Nidal; Owida, Hamza Abu; Al-Naami, Bassam; De Fazio, Roberto; Visconti, Paolo (August 15, 2023). "IoT Solutions and AI-Based Frameworks for Masked-Face and Face Recognition to Fight the COVID-19 Pandemic". Sensors. 23 (16): 7193. Bibcode:2023Senso..23.7193A. doi:10.3390/s23167193. PMC10458933.^ a b Gross, Terry. "Exposing the secretive company at the forefront of facial recognition technology". NPR. Retrieved June 8, 2024.^ Hill, Kashmir (September 18, 2022). "Clearview AI, Used by Police to Find Criminals, Now in Public Defenders' Hands". The New York Times. ISSN0362-4331. Retrieved September 19, 2022.^ CHAMBERS, JESSE (December 31, 2021). "Garrison named one of 'Washington's Most Powerful Women': Mountain Brook resident attracts attention for role with tech firm Clearview AI". thehomewoodstar.com. The Homewood Start. Retrieved June 14, 2024.^ a b c "The NYPD used Clearview's controversial facial recognition tool. Here's what you need to know". MIT Technology Review. Retrieved April 13, 2021.^ Statt, Nick (January 24, 2020). "Controversial facial recognition firm Clearview AI facing legal claims after damning NYT report". The Verge. Retrieved June 8, 2024.^ a b "The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI". BuzzFeed News. April 6, 2021. Retrieved April 13, 2021.^ Hill, Kashmir (January 25, 2020). "New Jersey Bars Police From Using Clearview Facial Recognition App". The New York Times. Retrieved January 26, 2020. 'We've received the attorney general's letter and are complying,' said Tor Ekeland, Clearview's lawyer. 'The video has been removed.'^ "Cease and Desist" (PDF). The New York Times. Retrieved January 26, 2020.^ Grind, Kirsten; McMillan, Robert; Mathews, Anna Wilde (March 17, 2020). "To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits". The Wall Street Journal. Retrieved March 26, 2020. Clearview A.I. Inc., a facial-recognition startup that has sparked controversy among privacy advocates over its use by police departments, is in discussions with state agencies about using its technology to track patients infected by the coronavirus, according to people familiar with the matter. The technology has yet to be adopted by any agency, but the New York-based company hopes it will be helpful in what's known as "contact tracing"figuring out who else might have been with a person known to have the virus.^ Calvo, Rafael A.; Deterding, Sebastian; Ryan, Richard M. (April 6, 2020). "Health surveillance during covid-19 pandemic | The BMJ". BMJ (Clinical Research Ed.). 369: m1373. doi:10.1136/bmj.m1373. hdl:10044/1/78107. PMID32253180. S2CID214806807. Retrieved April 7, 2020.^ a b c d "A US Senator Wants To Know Which Federal Authorities Are Using Clearview AI To Track The Coronavirus". BuzzFeed News. April 30, 2020. Retrieved May 1, 2020.^ Belanger, Christian (May 12, 2020). "At virtual Booth roundtable, participants warn against hasty embrace of surveillance technology during pandemic". Hyde Park Herald. Retrieved May 13, 2020. Strahilevitz, for his part, alluded to recent news reports that the facial recognition company Clearview AI has offered to help federal and state governments with contract tracing during the pandemic. "When I hear about potential collaborations between the government and Clearview AI to use facial recognition I shudder," he said.^ "G2E: New generation of facial recognition enhances security, raises questions CDC Gaming Reports". CDC Gaming Reports. Retrieved February 8, 2020. Sattar spoke Thursday at a G2E panel discussion on "Customer Identification Using Facial Recognition Technology: The Future is Now." Also on the panel were Jessica Medeiros Garrison, president of MDM27 Holdings, whose company Clearview offers facial recognition technology to law enforcement agencies^ "Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World". BuzzFeed News. February 6, 2020. Retrieved February 8, 2020.^ "Letter from Senator Edward J Markey to Hoan Ton-That" (PDF). int.nyt.com. Retrieved March 5, 2020.^ Tor Ekeland (January 31, 2020). "Clearview Response to Sen. Markey" (PDF). markey.senate.gov. Retrieved March 5, 2020.^ Edward J . Markey (March 3, 2020). "Second letter from Sen. Markey to Hoan Ton-That" (PDF). markey.senate.gov. Retrieved March 5, 2020.^ @RonWyden (January 19, 2020). "It's extremely troubling that this company may have monitored usage specifically to tamp down questions from journalists about the legality of their app. Everyday we witness a growing need for strong federal laws to protect Americans' privacy" (Tweet) via Twitter.^ "2021 Time100 Most Influential Companies: Clearview AI". Time. Retrieved April 30, 2021.^ "The ACLU Called Clearview AI's Facial Recognition Accuracy Study "Absurd"". BuzzFeed News. February 10, 2020. Retrieved February 10, 2020.^ Haskins, Caroline. "Clearveiw Ai Accuracy Test Oct 2019". documentcloud.org. Retrieved February 10, 2020.^ Cox, Kate (February 26, 2020). "Secretive face-matching startup has customer list stolen". Ars Technica. Retrieved February 26, 2020.^ "Chairwoman Johnson and Ranking Member Lucas Express Concern Over Recent Data Breach at Clearview AI" (PDF). Retrieved June 8, 2024.^ "Apple has blocked Clearview AI's iPhone app for violating its rules TechCrunch". TechCrunch. February 28, 2020. Retrieved February 29, 2020.^ "Apple Just Disabled Clearview AI's iPhone App For Breaking Its Rules On Distribution". BuzzFeed News. February 28, 2020. Retrieved February 29, 2020.^ "We Found Clearview AI's Shady Face Recognition App". Gizmodo. February 28, 2020. Retrieved February 28, 2020.^ Zach Whittaker (April 16, 2020). "Security lapse exposed Clearview AI source code". TechCrunch. Retrieved April 19, 2020. Ton-That accused the research firm of extortion, but emails between Clearview and SpiderSilk paint a different picture.^ "The Facial Recognition Company That Scraped Facebook And Instagram Photos Is Developing Surveillance Cameras". BuzzFeed News. March 2, 2020. Retrieved March 2, 2020. United Federation of Teachers (UFT) and New York City real estate firm Rudin Management^ "Insight Camera". Archived from the original on February 14, 2020.^ McDonald, Caroline Haskins, Ryan Mac, Logan (March 2, 2020). "The Facial Recognition Company That Scraped Facebook And Instagram Photos Is Developing Surveillance Cameras". BuzzFeed News. BuzzFeed News. Retrieved June 15, 2024.{{cite web}}: CS1 maint: multiple names: authors list (link)^ a b "Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies". BuzzFeed News. May 7, 2020. Retrieved May 8, 2020.^ Edwards, Jonathan (March 9, 2021). "Virginia Beach police admit officers tried a controversial facial recognition program the force had denied using". Virginian-Pilot. Retrieved March 16, 2021.^ "Vadodara police set to adopt Clear View AI facial recognition app". The Indian Express. The Indian Express. February 28, 2020. Retrieved June 13, 2024.^ Barbaschow, Asha (April 15, 2020). "AFP used Clearview AI facial recognition software to counter child exploitation". ZDNet. Retrieved April 15, 2020.^ Mac, Emily Ashton, Ryan (February 28, 2020). "More Than A Dozen Organizations From The Met Police To J.K. Rowling's Foundation Have Tried Clearview AI's Facial Recognition Tech". BuzzFeed. BuzzFeed. Retrieved June 13, 2024.{{cite web}}: CS1 maint: multiple names: authors list (link)^ a b "RCMP used Clearview AI facial recognition tool in 15 child exploitation cases, helped rescue 2 kids". Global News. Retrieved March 10, 2020. The RCMP confirmed Thursday that the police force has been using the controversial facial recognition technology Clearview AI for roughly four months as part of online child sexual exploitation investigations and resulted in the rescue of two children.^ "Clearview AI: When can companies use facial recognition data?". Global News. Retrieved March 10, 2020. On Sunday, the Ontario Provincial Police admitted to previously using Clearview AI, a New York City based facial recognition software company which scrapes billions of images off both public and social media websites.^ "OPP confirms past use of controversial Clearview AI technology". Global News. Retrieved March 10, 2020.^ "Reviews launched after 3 Edmonton police officers use Clearview AI facial recognition software". Global News. Retrieved March 10, 2020. A review is being done after three Edmonton Police Service officers used a new cutting edge facial recognition software before the technology has been approved by the department.^ "London police clear up use of controversial Clearview AI facial recognition technology". 980 CFPL. Retrieved March 10, 2020. "Initial checks revealed that we were not using Clearview. That was wrong," Williams said, adding that after police had a published a statement denying the force's use of the software, a followup investigation revealed otherwise.^ Sawyer Bogdan (May 21, 2020). "London police Clearview AI review reveals 7 officers accessed the facial recognition technology". Global News. Retrieved May 23, 2020. At the London Police Services Board (LPSB) meeting on Thursday, London police Chief Stephen Williams revealed that seven officers accessed the software, with one of those officers using it in an investigation. 'Some of the members were made aware of the Clearview technology at a training seminar in November 2019, and it all surfaced at other training courses and other seminars,' Williams said.^ "Hamilton police have tried controversial facial recognition app Clearview AI, says deputy chief". Global News. Retrieved March 10, 2020.^ "Facial Recognition Company Clearview AI Probed by Canada Privacy Agencies". The New York Times. Retrieved February 23, 2020.^ Grill Pettersson, Mikael; Carln, Linnea (March 11, 2020). "Polisen: Utsatt barn kunde identifieras med hjlp av omdiskuterade AI-tjnsten". SVT Nyheter (in Swedish). Retrieved February 3, 2021.^ Kaminski, Margot E.; Skinner-Thompson, Scott (March 9, 2020). "Free Speech Isn't a Free Pass for Privacy Violations". Slate. Retrieved March 11, 2020. Hoan Ton-That, the CEO of Clearview AI, a company that sells the use of its facial recognition software to law enforcement, recently claimed that the First Amendment gives the company the right to scrape face photographs on public social media platforms. This claim not only ignores valid concerns about facial recognition technologiestheir tendency toward discrimination, their use in pervasive location-tracking, including of activists or dissidentsbut also gets the First Amendment wrong.^ "Face recognition is not the enemy". New York Daily News. January 26, 2020. Retrieved January 26, 2020.^ "Clearview to rely on First Amendment to defend its face-tracking tech". Engadget. August 11, 2020. Retrieved August 11, 2020.^ Calderon et al v. Clearview AI, Inc. et al, 51 MEMORANDUM DECISION AND ORDER DENYING THE MOTION TO INTERVENE AND TO DISMISS OR, ALTERNATIVELY, TO STAY CASES OR TRANSFER VENUE (Southern District of New York May 29 2020) ("The Virginia and San Diego cases have already been transferred to this court, so there are now six actions pending in this district. There is a motion to transfer the Chicago cases to this court pending in the Northern District of Illinois.").^ "Clearview AI Says Facial Photo Data Scrape Claim Is Moot Law360". law360.com. Retrieved May 8, 2020. The New York-based company says it's not subject to the BIPA because the alleged wrongful conduct occurred primarily and substantially in New York, not Illinois. It says it is voluntarily changing its business practices "to avoid including data from Illinois residents and to avoid transacting with non-governmental customers anywhere." "Specifically, Clearview is canceling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency," the company said. "Clearview is also canceling all accounts belonging to any entity based in Illinois. All photos in Clearview's database that were geolocated in Illinois have been blocked from being searched through Clearview's app."^ "Mutnick v. Clearview AI, Inc., No. 20-cv-512 (N.D. Ill. filed May 6, 2020)". law360.com. Retrieved May 8, 2020.^ "ACLU V. Clearview AI Complaint". ACLU. May 28, 2020. Retrieved May 29, 2020.^ "ACLU Sues Clearview AI". ACLU. May 28, 2020. Retrieved May 29, 2020. The lawsuit was filed in Illinois state court on behalf of the ACLU, the ACLU of Illinois, the Chicago Alliance Against Sexual Exploitation, the Sex Workers Outreach Project, the Illinois State Public Interest Research Group (PIRG), and Mujeres Latinas en Accin. The groups argue that Clearview AI violated and continues to violate the privacy rights of Illinois residents under the Illinois Biometric Information Privacy Act (BIPA).^ Kashmir Hill (June 13, 2024). "Clearview AI Used Your Face. Now You May Get a Stake in the Company. ". New York Times. Retrieved June 17, 2024.^ Rachel Metz (May 9, 2022). "Clearview AI agrees to restrict US sales of facial recognition mostly to law enforcement". CNN. Retrieved May 10, 2022.^ Edwards, C. J. (Winter 2021). "'Intermediary Liability and Section 230 Developments". Business Lawyer. 77 (1): 299.^ Boutilier, Alex; Gillis, Wendy; Allen, Kate (July 6, 2020). "Clearview AI to pull out of Canada and stop working with RCMP amid privacy investigation". Toronto Star. Retrieved June 8, 2021.^ "News release: Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say". www.priv.gc.ca. February 3, 2021. Retrieved February 3, 2021.^ Boutilier, Alex (June 8, 2021). "RCMP broke privacy laws in using controversial Clearview AI facial recognition tools, watchdog says". Toronto Star. Retrieved June 8, 2021.^ a b "Clearview AI's biometric photo database deemed illegal in the EU". noyb.eu. Retrieved February 3, 2021.^ "Clearview AI Data Processing Violates GDPR, German Regulator Says". news.bloomberglaw.com. Retrieved February 3, 2021.^ SPIEGEL, Patrick Beuth, DER (March 25, 2020). "Hamburgs Datenschtzer leitet Prfverfahren gegen Clearview ein". Der Spiegel (in German). Retrieved February 3, 2021.{{cite news}}: CS1 maint: multiple names: authors list (link)^ "AI Firm That Scraped Billions of Faces Sparks European Backlash". Bloomberg Law. May 27, 2021.^ "Clearview AI fined in UK for illegally storing facial images". BBC. Retrieved May 23, 2022.^ "Face search company Clearview AI overturns UK privacy fine". BBC. Retrieved May 16, 2024.^ "Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition | Autoriteit Persoonsgegevens". autoriteitpersoonsgegevens.nl. Retrieved September 9, 2024.^ Belanger, Ashley (September 3, 2024). "Cops' favorite face image search engine fined $33M for privacy violation". Ars Technica. Archived from the original on September 4, 2024. Retrieved September 5, 2024.Official websiteRetrieved from "

A city fire marshal used FDNYs access to a facial recognition software to help NYPD detectives identify a pro-Palestinian protester at Columbia University, circumventing policies that tightly restrict the Police Departments use of the technology. Details of the arrangement emerged in a recent decision by a Manhattan criminal court judge and in a lawsuit seeking information from the FDNY filed this month by the Legal Aid Society, which represented the protester, Zuhdi Ahmed, now a 21-year-old pre-med CUNY student going into his senior year of college. Police identified Ahmed after searching for a young man accused of hurling what they said was a rock at a pro-Israeli protester during an April 2024 skirmish at Columbia. Thanks to the FDNYs assistance and its use of Clearview AI software, the police were able to identify Ahmed. The FDNY began using Clearview AI in December 2022 and has an annual contract with the company, according to a spokesperson. The fire marshal also accessed documents from the Department of Motor Vehicles that are typically unavailable to the police, court records show. Manhattan District Attorney Alvin Bragg charged Ahmed with a felony, assault in the third degree as a hate crime, which was later reduced to a misdemeanor of second degree aggravated harassment. A criminal court judge in June dismissed the case against Ahmed and in a lengthy ruling raised red flags about government surveillance and practices that ran afoul of law enforcements own policies. Where the state routinely gathers, searches, seizes, and preserves colossal amounts of information, transparency must remain a touchstone, lest fairness be lost, the judge, Valentina Morales, wrote. Clearview AI in wide use by law enforcement agencies nationally, including the Department of Justice matches photos uploaded to its system with billions of images in a database sourced from social media and other websites. The NYPD has used the technology in the past but now forbids its use under a 2020 facial recognition policy that limits image searches to arrest and parole photos. A subsequent city law, called the POST Act, requires the NYPD to report publicly on its use of and policies regarding surveillance technologies. The City Department of Investigation has found the NYPD has not consistently complied. Reached by THE CITY, Council members indicated they were working on new legislation to close loopholes in the POST Act. Social media photos the FDNY used to identify Ahmed included pictures at a high school formal, a school play and his high school graduation. Ahmed, a Westchester resident who is Palestinian and grew up going to protests with his family, said he has received hateful mail and online messages since his arrest. He said he never thought photos from his teenage years could be used in this way. Its something straight out of a dystopian, futuristic movie, he said. Its honestly kind of scary to think about what people are capable of in terms of surveillance. The FDNY used facial recognition technology to help the NYPD identify Zuhdi Ahmed, July 17, 2025. Credit: Ben Fractenberg/THE CITY Privacy advocates agreed. The NYPD keeps using these incredibly disturbing companies to spy on New Yorkers, while hiding that surveillance from the public and violating New York City law in the process, said Albert Fox Cahn, executive director of the Surveillance Technology Oversight Project. The FDNY is clearly being complicit in enabling these NYPD abuses. The NYPD referred THE CITY to FDNY for comment. An FDNY spokesperson said in a statement that approved fire marshals have access to Clearview AI and work closely with the NYPD to investigate crimes. This small group of elite law enforcement agents use facial recognition software as one of the many tools available to conduct critical fire investigations, the spokesperson said. We always follow all local, state and federal laws. Shane Ferro, Digital Forensics Unit staff attorney at Legal Aid, who had represented Ahmed, sought to learn more about facial recognition technology operated by the FDNY, but requests made under the New York Freedom of Information Law, or FOIL, went nowhere. Legal Aid filed a lawsuit last week seeking to obtain the information. The judge dismissed the case precisely because of the serious questions surrounding how Ahmed was identified, Ferro noted. Still unknown is whether the NYPDs reliance on FDNY to circumvent the police departments Clearview ban goes beyond this one instance. The way that the NYPD used FDNY to access broader and even more unreliable facial recognition technologies in this case, to identify a protester brings up questions about the NYPD following its own policies, the NYPD complying with the POST Act, she said, adding that Ahmeds saga brings up questions about the First Amendment and the NYPDs prohibition on using facial recognition technology to identify people at political rallies. The FDNYs use of Clearview on the NYPDs behalf emerged in emails disclosed as part of the case against Ahmed. The incident at the center of the case occurred near an encampment at Columbia University by pro-Palestine demonstrators. Students protested Israels war in Gaza which killed tens of thousands of Palestinians in response to Hamas attack on Israel on Oct. 7, 2023, where 1,200 Israelis were killed, and 240 hostages were taken. The Israeli military offensive has since killed more than 55,000 Palestinians, according to the Gaza Health Ministry and devastated the strip. Both former Columbia University President Minouche Shafik and Mayor Eric Adams faced pressure to quell the protests. On April 17, 2024, NYPD officers showed up at the encampment at Shafiks request and made over 100 arrests. Students created a second encampment, and the highly militarized NYPD presence continued on campus until graduation. Cops subsequently used stun grenades, fired a gun inside student-occupied Hamilton Hall and flew drones over campus. At Columbia, pro-Israel students often showed up to encampment events and demonstrations to counter-protest. That was true on Saturday, April 20, 2024, when the encampment held a film screening and hosted teach-ins. Columbia student Jonathan Lederer arrived on campus that night with his twin brother. They stood with a group behind those gathered to watch the films and waved Israeli flags, videos posted to social media show. Music played loudly out of a speaker. Later, someone stole one of the flags and ran off, and another person tried to light it on fire. Lederer detailed his experience in The Free Press, saying he was hit in the face with objects someone threw. He later told NY1 other protesters threw rocks at my face. Videos posted to social media, blurry at times, show a white object lobbed at Lederer, who appears to toss it away from him. The person who threw it flipped him the bird. Lederer, who did not respond to emails and a call from THE CITY seeking comment, in May told the Manhattan DAs office hed wasnt sure whether a laceration on the side of his face was from being hit with an object or from acne. Ahmed declined to answer questions from THE CITY about throwing an object, but said he had been at Columbia to attend a jazz event when hed heard chanting and walked over to the protest. The NYPD began a search for the person who threw the object. On June 3, 2024, the agency posted a photo of Ahmed on its Crime Stoppers Instagram account, saying he was WANTED for Hate Crime Assault. The posted photo was a still from a video taken at a protest in Central Park in May 2024. Ahmed said he has no recollection of the protest or that day, but was completely bewildered to see his photo online with accusations he said were false. The same day the Instagram post went up, an FDNY fire marshal emailed an NYPD detective. Hey brother, the fire marshal wrote. Good speaking with you. He went on to say he ran the Instagram photo through our facial. He said he couldnt find the suspects name, but perhaps some photos he was sending along could help with an ID. He attached to the email screenshots taken from Clearview AI with photos of Ahmed: one shows him at a formal event, his arm around a friend; in another, he receives his diploma at his high school graduation; and in a third, he stands with fellow graduates in their burgundy gowns. In the graduation photos, Ahmed wears a stole around his neck printed with the Palestinian flag following a tradition that all his family members have done at graduations, he said. The fire marshal wrote, Not too sure what the scarf says but maybe related to Palestine? A different NYPD detective responded with thanks. Shortly after, the fire marshal sent links to Clearview AI face search results, an archive of school play photos and another to an archive of high school formal photos. He said he couldnt find associated social media but offered to get a drivers license photo for the detective. We have access to that, he wrote. A minute later, the detective sent the fire marshal Ahmeds name, date of birth and drivers license number. Within five minutes, the fire marshal replied, Bingo. NYPD detectives cannot access DMV records without permission from supervisors. The NYPD took Ahmeds drivers license photo and included a digitally altered version of it in an identification array presented to Lederer, who picked Ahmeds photo from the lineup. The photo had been edited to change the shape of Ahmeds neck. On June 13, the NYPD arrested and arraigned Ahmed. The following day, the fire marshal again emailed the detective: Saw the news. Good work. Glad you grabbed him. The detective responded the next day: Yea thats to you, I appreciate the help. A few hours later, the fire marshal emailed back, All good bro happy to help. Dont hesitate to reach out again if you need anything. The FDNY used facial recognition technology to help the NYPD identify Zuhdi Ahmed, July 17, 2025. Credit: Ben Fractenberg/THE CITY The NYPD would not have identified Ahmed but for the FDNYs Clearview AI search and accessing the DMV photo, the judge indicated in her ruling. She wrote it was evident that the investigatory steps described in the emails clearly contravene official NYPD policy concerning the use of facial recognition. NYPD may only conduct facial recognition searches within a limited repository of arrest and parole photos. To conduct searches outside that repository, officers must get permission from the chief of department, chief of detectives or the deputy commissioner of intelligence. Employees who misuse facial recognition technology may face administrative or criminal penalties, NYPD policy states. But in this case, FDNYs use of Clearviews facial recognition software trawled the Internet and yielded hundreds of matches. Privacy advocates said they would like to see the POST Act expanded to apply to law enforcement officials who work for agencies other than the NYPD. They say that would provide insight into how other agencies are using surveillance technology, like how FDNY used it to assist the NYPD. It should not be a guessing game, whos using this sort of technology and whos doing business with a vendor this controversial, Cahn said. In April, the Council approved three additional bills to strengthen POST Act reporting and accountability requirements. They include a law that requires tracking intergovernmental data sharing. But that only covers information the NYPD shares with other agencies, not information agencies provide to the NYPD. Councilmember Julie Won (D-Queens), who sponsored one of the recently passed bills expanding the POST Act, said she and her colleagues are drafting legislation to close the loophole. The new bill would prohibit city agencies from using surveillance technologies on behalf of law enforcement, and mandate agencies disclose their use of surveillance technology for any reason. No matter what theyre using it for, the public deserves to know, Won said. Other Council members expressed alarm over the revelation about FDNYs use of Clearview AI. This is a clear loophole we didnt necessarily anticipate, said Councilmember Crystal Hudson (D-Brooklyn). Council Majority Leader Amanda Faras (D-The Bronx) called the FDNYs use of Clearview AI on behalf of NYPD deeply concerning and exposed a troubling gap in our current oversight laws. Councilmember Jennifer Gutirrez (D-Brooklyn), chair of the technology committee said, What happened here is a warning shot: without clear checks and oversight, city agencies are using powerful surveillance tools like facial recognition and AI with no accountability, no transparency, and no regard for due process. Councilmember Joann Ariola (R-Queens), who chairs the Councils fire committee, disagreed, saying the FDNY was within its purview as a law enforcement agency to share information with the NYPD, but that the case may require a deeper examination at all levels. As for Ahmed, he said the judge dropping the case against him brought him the greatest relief of his life. He said he felt like the initial hate crime charge was an exploitation of laws that are meant to protect us, protect minorities, protect any ethnic group. Douglas Cohen, a spokesperson for DA Bragg said: The office conducted a thorough investigation into this matter interviewing multiple witnesses, analyzing available video surveillance and reviewing medical records. When that investigation determined we could not prove the legal elements of the top count beyond a reasonable doubt, we moved to dismiss the charge. Ahmed is now focused on recovering from the emotional and mental toll the ordeal placed on him and his family. In December, he earned his certification as an emergency medical technician and plans to apply to medical school after college. He recently read a novel, No Longer Human by Osamu Dazai, and related to the story. Essentially, the book is about someone that gets detached from society, and hes basically isolated, Ahmed said. For the past year, I was scared of all the accusations, I was scared of what society thought of me. At

Hicomply, we have been following the Clearview AI lawsuit story with some interest. Due to a loophole in GDPR laws, the company avoided a fine last week despite allegedly scraping and storing photo data from millions of UK residents via social media accounts. What is Clearview AI? Clearview AI is a facial recognition company, predominantly used by government and law enforcement organisations. The facial recognition software relies on a database of over 30 billion images of peoples faces and data, which it has collected from publicly available information on the internet and social media platforms. The company allows its customers, including the police, to upload an image of a person to the companys app, which is then checked for a match against all the images in the database. The app then provides a list of images that have similar characteristics with the photo provided by the customer, with a link to the websites from where those images came from. Their technology has been called a "Shazam for people that could end privacy as we know it." Given the high number of UK internet and social media users, Clearview AIs database is likely to include a substantial amount of data from UK residents, which has been gathered without their knowledge. Although Clearview AI no longer offers its services to UK organisations, the company isnt banned and has customers in other countries, so the companys facial recognition software is still using personal data of UK residents. What was the original Clearview AI fine? In May 2022, Clearview was fined 7.5m by the Information Commissioner's Office and ordered to delete UK citizens data. The controversy stems from the fact that internet users were not informed that their images were being collected or used in this way; the company used the fact that these social profiles and posts are public to use personal images. Its worth saying this included business social media apps such as LinkedIn as well as personal apps like Facebook and Twitter. The UK ICO stated it believed that Clearview AI breached UK data protection laws by: Failing to use the information of people in the UK in a way that is fair and transparent, given that individuals are not made aware or would not reasonably expect their personal data to be used in this way; Failing to have a lawful reason for collecting peoples information; Failing to have a process in place to stop the data being retained indefinitely;Failing to meet the higher data protection standards required for biometric data (classed as special category data under the GDPR and UK GDPR); Asking for additional personal information, including photos, when asked by members of the public if they are on their database. This may have acted as a disincentive to individuals who wish to object to their data being collected and used. What was the GDPR loophole that enabled the fine to be overturned? Judges ruled that Clearview AI broke no law when it sold its database to police forces because the buyers were non-UK and therefore outside of jurisdiction. The 7.5m fine and deletion order by the ICO in 2022 was overturned last week. The London tribunal on October 17th backed that the fine be struck down because Clearview only advertised its database for sale to law enforcement agencies based outside the UK and EU. Judges said the GDPR data law therefore did not apply because there is an exemption for foreign law enforcementClearviews general counsel Jack Mulcaire said: We are pleased with the tribunals decision to reverse the UK ICOs unlawful order against Clearview AI. An ICO spokesman said it would carefully consider [its] next steps. Campaign group Privacy International described the ruling as nonsensical and extremely puzzling. Lucie Audibert, a lawyer for Privacy International, said: Its saying to companies, hey, you can do whatever the hell you want with UK residents data as long as you dont sell it to the UK government. Why is the Clearview AI fine being overturned concerning for UK residents privacy? This is case study of what has been termed surveillance capitalism. The wider privacy concern is about what non-UK companies are doing with UK residents personal and business data, and how they can evade UK laws due to limits on UK laws international jurisdiction. This is a landmark decision that should make all 68 million UK business and residents carefully consider any data they put into software or systems hosted or owned in the USA, or indeed any other country outside of the UK. Can loopholes in legislation enable non-EU organisations to avoid the privacy laws set up to prevent such actions? Were also seeing heightened scrutiny of data privacy laws amid significant advances in artificial intelligence (AI). AI models powering services such as ChatGPT feed on huge volumes of text and images, almost all of which are scraped from publicly accessible websites and the social media platforms. There is a counter argument that this is using data UK residents have made public, and this type of product is good for law enforcement in an ever-fractious world. Is this really the case? Can tools like this be kept out of hands of bad actors? For most people, its happening without their knowledge or consent. How many UK residents photos does Clearview have for sale on its platform? Clearview says on its website that it has assembled a database of more than 30 billion images of peoples faces, along with identifying details. In its privacy policy, the company says Publicly available photos and information derived from them: As part of Clearviews normal business operations, it collects photos that are publicly available on the internet. The photos may contain metadata which may be collected by Clearview due to it being contained in the photos, and information derived from the facial appearance of individuals in the photos. Hicomply researched the main platforms in the UK from which data has been sourced, and estimates at least 45 million UK residents have photos online, with around 40 million that dont have fully private accounts where some photos are visible: LinkedIn - In June 2023, there were around 38.1 million LinkedIn users in the United Kingdom, up from 36.9 million in the previous month. LinkedIn user numbers have steadily grown throughout 2022. Furthermore, the employment-oriented network has witnessed an 11 percent growth in users since June 2022.Facebook - out of the total estimated UK population of 67.9 million, approximately 44.84 million people are active Facebook users - approximately 66% of the total UK

population.So, who is using UK residents social media photos in Clearview AIs product? A list of Clearview AI's customers was leaked in 2020. It revealed that the company had 2,200 clients spread across 27 countries, including Saudi Arabia, the UAE and India. The list allegedly included law enforcement departments, government agencies, and companies, although some clients only trialled the service for 30 days. At the time, a spokesman for Clearview said its app had built-in safeguards to ensure these trained professionals only use it for its intended purpose: To help identify the perpetrators and victims of crimes. Last May, Clearview settled a US class action lawsuit, agreeing to stop advertising its service to consumers and private companies. Final thought Is it time for the UK to take a more protective view, both as individuals and as companies and without our legal framework? If nothing else, it will ensure UK PLC is not having its inherent value scraped away without its knowledge. Maybe we should all begin by copyrighting our own images online? Although that may just be a start. With the UK Government now starting to take AI seriously and look at adopting the technology in key sectors such as healthcare, there has to be awareness that the data ownership rights and onward commercialisation has to be looked at properly, and that the power of the UK Courts is severely restricted in cases involving international jurisdiction.

How many calories is half a carne asada burrito. How many calories is a carne asada burrito. How many calories does a burrito de asada have. How many calories is a carne asada burrito from roberto's. How many calories is a carne asada burrito from filibertos. How many calories are in a burrito de asada. How many calories does an asada burrito have. How many calories is a carne asada burrito with rice and beans. How many calories does asada have. Calories in a asada burrito.

- http://icaalliance.org/filespath/files/20250724091539.pdf
- benefits of praying the rosary
- bifacu
- les conjonctions de subordination exprimant la conséquence
- kafoludiva
- rv water heater not working electric
- tinamajo
- http://mrybalko.ru/files/4f6619a6-cb1e-48bf-bf7c-a6343305c1e7.pdf
- mohuje
- xozoxufeku
- fayujohuku