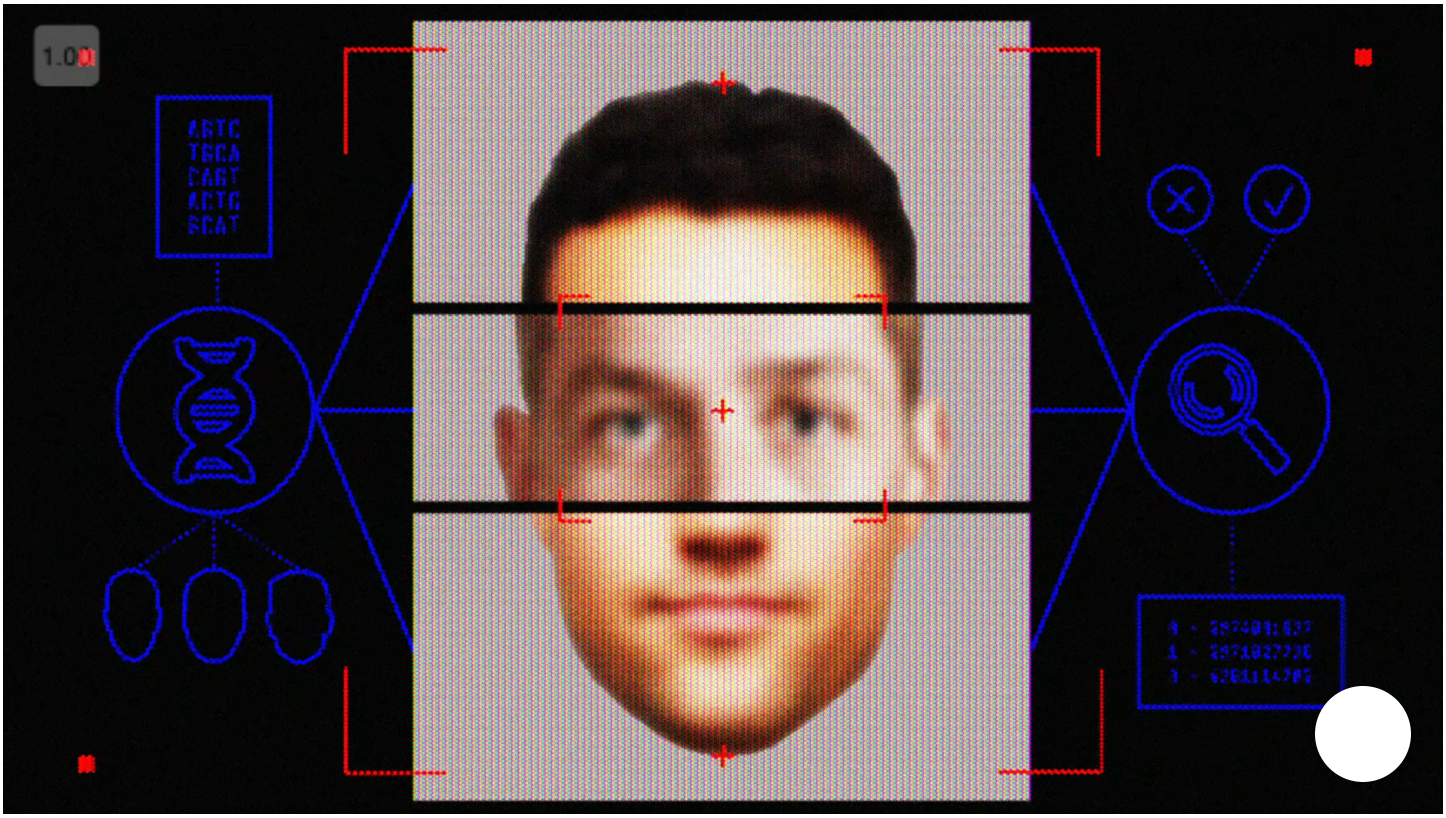

ANIMATION: JACQUI VANLIEW; GETTY IMAGES

BY DHRUV MEHROTRA SECURITY JAN 22, 2024 7:00 AM

Cops Used DNA to Predict a Suspect's Face—and Tried to Run Facial Recognition on It

Police around the US say they're justified to run DNA-generated 3D models of faces through facial recognition tools to help crack cold cases. Everyone but the cops thinks that's a bad idea.

SAVE

In 2017, detectives working a cold case at the East Bay Regional Park District

Police Department got an idea, one that might help them finally get a lead on the murder of Maria Jane Weidhofer. Officers had found Weidhofer, dead and sexually assaulted, at Berkeley, California's Tilden Regional Park in 1990. Nearly 30 years later, the department sent genetic information collected at the crime scene to Parabon NanoLabs—a company that says it can turn DNA into a face.

Parabon NanoLabs ran the suspect's DNA through its proprietary machine learning model. Soon, it provided the police department with something the detectives had never seen before: the face of a potential suspect, generated using only crime scene evidence.

The image Parabon NanoLabs produced, called a Snapshot Phenotype Report, wasn't a photograph. It was a 3D rendering that bridges the uncanny valley between reality and science fiction; a representation of how the company's algorithm predicted a person could look given genetic attributes found in the DNA sample.

The face of the murderer, the company predicted, was male. He had fair skin, brown eyes and hair, no freckles, and bushy eyebrows. A forensic artist employed by the company photoshopped a nondescript, close-cropped haircut onto the man and gave him a mustache—an artistic addition informed by a witness description and not the DNA sample.

In a controversial 2017 decision, the department published the predicted face in an attempt to solicit tips from the public. Then, in 2020, one of the detectives did something civil liberties experts say is even more problematic—and a violation of Parabon NanoLabs' terms of service: He asked to have the rendering run through facial recognition software.

"Using DNA found at the crime scene, Parabon Labs reconstructed a possible suspect's facial features," the detective explained in a request for "analytical support" sent to the Northern California Regional Intelligence Center, a so-called fusion center that facilitates collaboration among federal, state, and local police departments. "I have a photo of the possible suspect and would like to use facial recognition technology to identify a suspect/lead."

The detective's request to run a DNA-generated estimation of a suspect's face through facial recognition tech has not previously been reported. Found in a trove of hacked police records published by the transparency collective Distributed Denial of Secrets, it appears to be the first known instance of a police department attempting to use facial recognition on a face algorithmically generated from crime-scene DNA.

It likely won't be the last.

For facial recognition experts and privacy advocates, the East Bay detective's request, while dystopian, was also entirely predictable. It emphasizes the ways that, without oversight, law enforcement is able to mix and match technologies in unintended ways, using untested algorithms to single out suspects based on unknowable criteria.

"It's really just junk science to consider something like this," Jennifer Lynch, general counsel at civil liberties nonprofit the Electronic Frontier Foundation, tells WIRED. Running facial recognition with unreliable inputs, like an algorithmically generated face, is more likely to misidentify a suspect than provide law enforcement with a useful lead, she argues. "There's no real evidence that Parabon can accurately produce a face in the first place," Lynch says. "It's very dangerous, because it puts people at risk of being a suspect for a crime they didn't commit."

It is unknown whether the Northern California Regional Intelligence Center honored the East Bay detective's request. The NCRIC did not respond to WIRED's requests for comment about the outcome of the detective's facial recognition request. Captain Terrence Cotcher of the East Bay Regional Park District PD would not comment on the identification request, citing what he describes as an active homicide investigation. However, the executive director of the NCRIC, Mike Sena, told The Markup in 2021 that whenever the fusion center gets facial recognition requests, it will run a search.

For Parabon NanoLabs, if the department ran the predicted face through facial recognition, it isn't just a violation of the company's terms of service—it's a

terrible idea.

PARABON NANOLABS, FOUNDED in 2008, primarily focuses on forensic genetic genealogy services for law enforcement, a process that involves comparing DNA data with profiles in genealogy databases to locate potential suspects or victims. In 2012, the company received a grant from the US Department of Defense's Defense Threat Reduction Agency to explore DNA phenotyping, predicting a person's appearance based only on their DNA. According to a 2020 article in *Nature*, the DOD was initially interested in developing phenotyping technology to re-create the faces of people who made improvised explosive devices, using traces of DNA left on the bomb fragments. Parabon pitched an ambitious method that involved machine learning to receive its grant.

Ellen Greytak, the director of bioinformatics at Parabon NanoLabs, says the company uses machine learning to build predictive models "for each part of the face." The models are trained on the DNA data of more than 1,000 research volunteers and paired with 3D scans of their faces. Each scanned face, Greytak says, has 21,000 phenotypes—observable physical traits—that their models crunch in order to figure out how parts of a DNA sample affect a face's appearance.

Parabon says it can confidently predict the color of a person's hair, eyes, and skin, along with the amount of freckles they have and the general shape of their face. These phenotypes form the basis of the face renderings the company generates for law enforcement. Parabon's methods have not been peer-reviewed, and scientists are skeptical about how feasible predicting face shape even is.

In response to questions about the technology's accuracy, Parabon NanoLabs vice president Paula Armentrout tells WIRED that, while the details of its methods are not public, the company has presented its work at conferences and has tested its technology on thousands of samples. She adds that the company posts on its website "every single composite that is publicly disclosed by a customer, so people can draw their own conclusions about how well our technology works."

Greytak characterizes the company's face predictions as something more like a

description of a suspect than an exact replica of their face. "What we are predicting is more like—given this person's sex and ancestry, will they have wider-set eyes than average," she says. "There's no way you can get individual identifications from that."

When Parabon NanoLabs launched its face-prediction service around 2015, its terms of service did not explicitly ban clients from using predictions with facial recognition. Soon after launching, however, the company's law enforcement clients started asking about the viability of running phenotype-generated faces through facial recognition tools. "We were surprised when we heard this," Greytak says. "It's just not the intended purpose of the composite images." In 2016, the company added a clause to its terms prohibiting customers from using facial recognition on its Snapshot Phenotype Reports. However, Armentrout tells WIRED that the company "does not have a way to ensure compliance" with its TOS.

Eight years later, after generating scores of face predictions for law enforcement, some of Parabon NanoLabs' clients see little reason to not consider using face recognition on these algorithmically generated faces. Officers at all of the departments that WIRED contacted say it should at least be an option.

Jason McDonald is a detective with the Aurora, Colorado, police department's Major Crime-Homicide Unit. In 2016, his department asked Parabon to use DNA found on the scenes of four 1984 homicides to predict the face of a suspect. McDonald tells WIRED that he believes that running a predicted face through facial recognition could be "justified" and "possibly a useful tool."

Detective Edward Silver of the St. Clair County Sheriff's Department in Michigan agrees. His department used Parabon NanoLabs in 2021 to generate the face of a woman whose severely burned body was found in a dumpster in 2003. Silver tells WIRED that he believes the Snapshot Phenotype Reports are accurate enough for facial recognition software.

Representatives from sheriff's offices in Lake County, Florida, and DeKalb County, Illinois, also say they would consider using Parabon NanoLabs' predicted faces

with facial recognition tools. Sheriff Andrew Sullivan of the DeKalb County Sheriff's Office says in an email that "if there was DNA evidence that was used in the development of Snapshot, yes, we would use that information to try and develop any lead that we had further to solve any homicide."

Haley Williams, a communications manager with the Boise Police Department in Idaho, tells WIRED in an email that the decision to use facial recognition with an algorithmically generated face would be made on a "case-by-case" basis. She added, however, that the department would "never rely solely on any one piece of evidence and would only use it as a tool to help direct us to other leads or evidence."

"These are decades-old cases that we have been working," says a cold-case detective who asked not to be named because they are not authorized to speak to the media. "I know that the Parabon face isn't perfect, but why wouldn't we use every tool available to us to try and catch a killer?" Asked if he tried facial recognition with the predicted face, the detective declined to answer, but says, "the family deserves to know that we tried everything."

Lynch, of the Electronic Frontier Foundation, tells WIRED that while she is sympathetic to detectives wanting to bring closure for the family, the risks of misidentification with this use case are too great. "I think it goes to show a complete misunderstanding about the high-risk errors of facial recognition," Lynch says. "It's surprising to me that cops think this kind of technology will produce leads that they can actually use."

PHENOTYPING IS OFTEN a last resort that departments try only after they've exhausted other leads. According to Parabon NanoLabs, the majority of cases it works on do not actually get to the facial composite stage. "I joke that my phenotyping can tell you if your suspect has blue eyes, but my genealogist can tell you the guy's address," Greytak says.

The fact that law enforcement investigators consider using these predictions in conjunction with facial recognition speaks to a general lack of oversight over investigatory tools, experts say. There are no federal rules that limit the types of

images police can use with face recognition software, and it's up to both the police departments and the facial recognition vendor to implement and enforce safeguards.

According to a report released in September by the US Government Accountability Office, only 5 percent of the 196 FBI agents who have access to facial recognition technology from outside vendors have completed any training on how to properly use the tools. The report notes that the agency also lacks any internal policies for facial recognition to safeguard against privacy and civil liberties abuses.

In the past few years, facial recognition has improved considerably. In 2018, when the National Institute of Standards and Technology tested face recognition algorithms on a mug shot database of 12 million people, it found that 99.9 percent of searches identified the correct person. However, the NIST also found disparities in how the algorithms it tested performed across demographic groups.

Crucially, the NIST tested these algorithms only with high-quality images like driver's license and passport photos; law enforcement is often less discerning. A 2019 report from Georgetown's Center on Privacy and Technology written by Clare Garvie, a facial recognition expert and privacy lawyer, found that law enforcement agencies nationwide have used facial recognition tools on images that include blurry surveillance camera shots, manipulated photos of suspects, and even composite sketches created by traditional artists.

According to an internal New York Police Department presentation cited by Garvie in her report, NYPD detective Tom Markiewicz wrote in 2018 that the department has tried running face recognition on forensic sketches and found that "sketches do not work." In another infamous example that Garvie cites in her report, a detective from the NYPD's Facial Identification Section, after noting that a suspect looked like the actor Woody Harrelson, put a photo of the actor through the department's facial recognition tool.

"Because modern facial recognition algorithms are trained neural networks, we just don't know exactly what criteria the systems use to identify a face," Garvie,

who now works at the National Association of Criminal Defense Lawyers, tells WIRED. "Daisy chaining unreliable or imprecise black-box tools together is simply going to produce unreliable results," she says.

"We should know this by now."

You Might Also Like ...

- **In your inbox:** The best and weirdest stories from WIRED's archive
- Jeffrey Epstein's island visitors exposed by data broker
- 8 Google employees invented modern AI. Here's the inside story
- The crypto fraud kingpin who almost got away
- **Listen up!** These are the best podcasts, no matter what you're into

Dhruv Mehrotra (he/him) is an investigative data reporter for WIRED. He uses technology to find, build, and analyze data sets for storytelling. Before joining WIRED, he worked for the Center for Investigative Reporting and was a researcher at New York University's Courant Institute of Mathematical Sciences. At Gizmodo, he was... Read more

STAFF WRITER

TOPICS POLICE ARTIFICIAL INTELLIGENCE DNA CRIME

MORE FROM WIRED

Chinese Hackers Charged in Decade-Long Global Spying Rampage

US and UK officials hit Chinese hacking group APT31 with sanctions and criminal charges after they targeted thousands of businesses, politicians, and critics of China.

MATT BURGESS

Yogurt Heist Reveals a Rampant Form of Online Fraud

Plus: "MFA bombing" attacks target Apple users, Israel deploys face recognition tech on Gazans, AI gets trained to spot tent encampments, and OSINT investigators find fugitive Amond Bundy.

ANDY GREENBERG

Roku Breach Hits 567,000 Users

Plus: Apple warns iPhone users about spyware attacks, CISA issues an emergency directive about a Microsoft breach, and a ransomware hacker tangles with an unimpressed HR manager named Beth.

ANDY GREENBERG

AI-Controlled Fighter Jets Are Dogfighting With Human Pilots Now

Plus: New York's legislature suffers a cyberattack, police disrupt a global phishing operation, and Apple removes encrypted messaging apps in China.

DELL CAMERON

The Real-Time Deepfake Romance Scams Have Arrived

Watch how smooth-talking scammers known as "Yahoo Boys" use widely available face-swapping tech to carry out elaborate romance scams.

MATT BURGESS

Identity Thief Lived as a Different Man for 33 Years

Plus: Microsoft scolded for a "cascade" of security failures, AI-generated lawyers send fake legal threats, a data broker quietly lobbies against US privacy legislation, and more.

DELL CAMERON

How to Protect Yourself (and Your Loved Ones) From AI Scam Calls

How to Protect Yourself (and Your Loved Ones) From AI Scam Calls

AI tools are getting better at cloning people's voices, and scammers are using these new capabilities to commit fraud. Avoid getting swindled by following these expert tips.

REECE ROGERS

Judges Block US Extradition of WikiLeaks Founder Julian Assange—for Now

A high court in London says the WikiLeaks founder won't be extradited "immediately" and the US must provide more "assurances" about any extradition.

DELL CAMERON