Cops Running DNA-Manufactured Faces Through Face Recognition Is a Tornado of Bad Ideas

In keeping with law enforcement's grand tradition of taking antiquated, invasive, and oppressive technologies, making them digital, and then calling it innovation, police in the U.S. recently combined two existing dystopian technologies in a brand new way to violate civil liberties. A police force in California recently employed the new practice of taking a DNA sample from a crime scene, running this through a service provided by US company Parabon NanoLabs that guesses what the perpetrators face looked like, and plugging this rendered image into face recognition software to build a suspect list.

Parts of this process aren't entirely new. On more than one occasion, police forces have been found to have fed images of celebrities into face recognition software to generate suspect lists. In one case from 2017, the New York Police Department decided its suspect looked like Woody Harrelson and ran the actor's image through the software to generate hits. Further, software provided by US company Vigilant Solutions enables law enforcement to create "a proxy image from a sketch artist or artist rendering" to enhance images of potential suspects so that face recognition software can match these more accurately.

Since 2014, law enforcement have also sought the assistance of Parabon NanoLabs—a company that alleges it can create an image of the suspect's face from their DNA. Parabon NanoLabs claim to have built this system by training machine learning models on the DNA data of thousands of volunteers with 3D scans of their faces. It is currently the only company offering phenotyping and only in concert with a forensic genetic genealogy investigation. The process is yet to be independently audited, and scientists have affirmed that predicting face shapes—particularly from DNA samples—is not possible. But this has not stopped law enforcement officers from seeking to use it, or from running these fabricated images through face recognition software.

Simply put: police are using DNA to create a hypothetical and not at all accurate face, then using that face as a clue on which to base investigations into crimes. Not only is this full dice-roll policing, it also threatens the rights, freedom, or even the life of whoever is unlucky enough to look a little bit like that artificial face.

But it gets worse.

In 2020, a detective from the East Bay Regional Park District Police Department in California asked to have a rendered image from Parabon NanoLabs run through face recognition software. This 3D rendering, called a Snapshot Phenotype Report, predicted that—among other attributes—the suspect was male, had brown eyes, and fair skin. Found in police records published by Distributed Denial of Secrets, this appears to be the first reporting of a detective running an algorithmically-generated rendering based on crime-scene DNA through face recognition software. This puts a second layer of speculation between the actual face of the suspect and the product the police are using to guide investigations and make arrests. Not only is the artificial face a guess, now face recognition (a technology known to misidentify people) will create a "most likely match" for that face.

These technologies, and their reckless use by police forces, are an inherent threat to our individual privacy, free expression, information security, and social justice. Face recognition tech alone has an egregious history of misidentifying people of color, especially Black women, as well as failing to correctly identify trans and nonbinary people. The algorithms are not always reliable, and even if the technology somehow had 100% accuracy, it would still be an unacceptable tool of invasive surveillance capable of identifying and tracking people on a massive scale. Combining this with fabricated 3D renderings from crime-scene DNA exponentially increases the likelihood of false arrests, and exacerbates existing harms on communities that are already disproportionately over-surveilled by face recognition technology and discriminatory policing.

There are no federal rules that prohibit police forces from undertaking these actions. And despite the detective's request violating Parabon NanoLabs' terms of service, there is seemingly no way to ensure compliance. Pulling together criteria like skin tone, hair color, and gender does not give an accurate face of a suspect, and deploying these untested algorithms without any oversight places people at risk of being a suspect for a crime they didn't commit. In one case from Canada, Edmonton Police Service issued an apology over its failure to balance the harms to the Black community with the potential investigative value after using Parabon's DNA phenotyping services to identify a suspect.

EFF continues to call for a complete ban on government use of face recognition —because otherwise these are the results. How much more evidence do law

markers need that police cannot be trusted with this dangerous technology? How many more people need to be falsely arrested and how many more reckless schemes like this one need to be perpetrated before legislators realize this is not a sustainable method of law enforcement? Cities across the United States have already taken the step to ban government use of this technology, and Montana has specifically recognized a privacy interest in phenotype data. Other cities and states need to catch up or Congress needs to act before more people are hurt and our rights are trampled.

TAGS:

DNA FACE RECOGNITION

RELATED UPDATES

California's Facial Recognition Bill Is Not the Solution We Need