The New York Times | https://nyti.ms/2EZcof2

How Facial Recognition Makes You Safer

Used properly, the software effectively identifies crime suspects without violating rights.

By James O'Neill
Mr. O'Neill is the New York police commissioner.

June 9, 2019

In 1983, when I was sworn in as a police officer, many of the routine tasks of the trade would have seemed more familiar to a cop from my grandfather's day than to a new police academy graduate today. I took ink fingerprints on paper cards and used a Polaroid camera for mug shots. Reports were handwritten or typed on carbon triplicates. Biological evidence could be analyzed only in terms of blood type.

Technology has improved the profession beyond what the most imaginative officer could have conceived in those days. These innovations include facial recognition software, which has proved its worth as a crime-fighting resource since we adopted it in 2011. But the technology has also raised concerns about privacy, so the public should know how the New York Police Department uses its system — and the safeguards we have in place.

When detectives obtain useful video in an investigation, they can provide it to the Facial Identification Section, of the Detective Bureau. An algorithm makes a template of the face, measuring the shapes of features and their relative distances from each other. A database consisting solely of arrest photos is then searched as the sole source of potential candidates — not photos from the Department of Motor Vehicles, Facebook, traffic cameras or the myriad streams of close-circuit TV video from around the city. Facial "landmarks" are compared without reference to race, gender or ethnicity.

After the software generates a list of possible matches, an investigator assesses their resemblance to the suspect. If one is selected, a review is conducted by detectives and seasoned supervisors, noting similarities and differences. If they affirm the match, the investigator proceeds with further research, including an examination of social media and other open-source images.

We might find social media images of a person at a birthday party wearing the same clothing as the suspect in a robbery. That person then becomes a lead; the facial identification team will provide only a single such lead to the case detective. Leads provided by the unit are comparable to tips to our Crime Stoppers hotline — no matter how compelling, they must be verified to establish probable cause for an arrest. No one can be arrested on the basis of the computer match alone.

In 2018, detectives made 7,024 requests to the Facial Identification Section, and in 1,851 cases possible matches were returned, leading to 998 arrests. Some investigations are still being conducted and some suspects have not been apprehended.

But in many cases there have been clear results. Recently, the work of the facial identification team led to the arrest of a man accused of raping a worker at a day spa, and another charged with pushing a subway passenger onto the tracks. We have made arrests in murders, robberies and the on-air assault of a TV reporter. A woman whose dismembered body was found in trash bags in two Bronx parks was identified. So was a woman hospitalized with Alzheimer's, through an old arrest photo for driving without a license.

The software has also cleared suspects. According to the Innocence Project, 71 percent of its documented instances of false convictions are the result of mistaken witness identifications. When facial recognition technology is used as a limited and preliminary step in an investigation — the way our department uses it — these miscarriages of justice are less likely.

We have never put police sketches into the system; they would be of no value. We have used editing software to substitute a generic feature when a suspect is closing his eyes or sticking out his tongue in the submitted photo. The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3-D model.

[If you use technology, someone is using your information. We'll tell you how — and what you can do about it. Sign up for our limited-run newsletter.]

We use these methods solely to fill in missing or distorted data. And when we do so, we bring an additional degree of scrutiny to the process. To compare this to filling in a partial fingerprint, as the Georgetown Center for Privacy and Technology did in a recent report, is absurd. It makes sense to create an image of a suspect's left ear using his right ear as a model. But it is impossible to infer the shape of a nose from the shape of a chin. As the algorithm is constantly improving in its ability to read lower-quality images, the editing software is used less and less frequently.

The department does not conduct civil immigration enforcement, and neither does our Facial Identification Section. But we do work with other police departments when appropriate. A recent request from the F.B.I. led to the identification of a child sex trafficker who advertised his services on social media.

Biometric technology is no longer new. It is routinely used everywhere from shopping malls to doctors' offices. Its application by the department is carefully controlled and its invaluable contributions to police investigations have been achieved without infringement on the public's right to privacy. When cases using this technology have been prosecuted, our methods and findings are subject to examination in court.

Facial recognition technology can provide a uniquely powerful tool in our most challenging investigations: when a stranger suddenly commits a violent act on the street. In the days of fingerprint cards and Polaroid mug shots, these crimes defined New York City, for visitors and residents alike.

Though far rarer now, they remain life-altering, and sometimes life-ending, events. To keep New York City safe requires enormous and relentless effort. It would be an injustice to the people we serve if we policed our 21st-century city without using 21st-century technology.

James O'Neill is the police commissioner for New York City.

Follow @privacyproject on Twitter and The New York Times Opinion Section on Facebook and Instagram.