

The New York Times

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

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.

Like other media companies, The Times collects data on its visitors when they read stories like this one. For more detail please see our [privacy policy](#) and our [publisher's description of The Times's practices and continued steps to increase transparency and protections](#).

Follow [@privacyproject](#) on Twitter and [The New York Times Opinion Section](#) on Facebook and Instagram.

A version of this article appears in print on June 10, 2019, on Page A23 of the New York edition with the headline: How Facial Recognition Makes You Safer

READ 270 COMMENTS